

Workstation User's Manual

Workstation 6.5

BETA



Workstation User's Manual

Revision: 20080111

Item: WS6-ENG-Q207-296

You can find the most up-to-date technical documentation on our Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 1998-2008 VMware, Inc. All rights reserved. Protected by one or more U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, and 7,290,253; patents pending.

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.

3401 Hillview Ave.

Palo Alto, CA 94304

www.vmware.com

Contents

Preface 19

Introduction and System Requirements 24

Product Benefits 24

Overview of This Manual 25

About the Host and Guest Computers 26

Host System Requirements 26

PC Hardware 26

Memory 27

Display 27

Disk Drives 27

Local Area Networking (Optional) 28

Host Operating System 28

Virtual Machine Specifications 32

Processor 32

Chip Set 33

BIOS 33

Memory 33

Graphics 33

IDE Drives 33

SCSI Devices 33

Floppy Drives 34

Serial (COM) Ports 34

Parallel (LPT) Ports 34

USB ports 34

Keyboard 34

Mouse and Drawing Tablets 34

Ethernet Card 35

Sound 35

Virtual Networking 35

Supported Guest Operating Systems 35

Support for 64-Bit Guest Operating Systems 38

Installing VMware Workstation 39

- Installation Prerequisites 39
- Sharing a Workstation Host with Other VMware Products 40
- Install Workstation on a Windows Host 41
 - Install Workstation Silently 43
 - Uninstall Workstation from a Windows Host 44
- Install Workstation on a Linux Host 45
 - Configuring Workstation with vmware-config.pl 47
 - Uninstall Workstation from a Linux Host 48
- Where to Go Next 49

Upgrading Workstation and Virtual Machines 51

- Prepare for the Upgrade 51
- Removing Workstation 2 or 3 to Install Workstation 6.x 52
- Upgrade Workstation on a Windows Host 53
 - Upgrading to a Windows Vista Host 54
- Upgrade Workstation on a Linux Host 55
- Using an Older-Version Virtual Machine Without Upgrading 56
- Change the Version of the Virtual Machine 57

Learning Workstation Basics 61

- Start Workstation on a Windows Host 61
- Start Workstation on a Linux Host 62
- Overview of the Workstation Window 62
 - Home Page and Views 64
 - Toolbar Buttons 67
 - View the Sidebar 72
 - Favorites List in the Sidebar 72
- Check for Product Updates 74
- Quickly Create a Virtual Machine 75
- Introduction to Workstation Preferences 76
- Introduction to Virtual Machine Settings 79
 - Hardware Tab 79
 - Options Tab 80
- Closing Virtual Machines and Exiting Workstation 81
 - Set a Virtual Machine to Run in the Background 82
- Keyboard Shortcuts 82

Creating a Virtual Machine	85
Methods of Creating Virtual Machines	85
Configuration Options for the New Virtual Machine Wizard	86
Easy Install Feature for Windows Guest Operating Systems	86
Typical Versus Custom Configurations	87
Guest Operating System Selection	88
Virtual Machine Location	88
Number of Processors	89
Network Connection Type	89
SCSI Adapter Types	90
Normal and Independent Disk Modes	90
Virtual Disks and Physical Disks	91
Disk Capacity	91
Pocket ACE Disk Size Calculator on Windows Only	91
Using the New Virtual Machine Wizard	92
Create a Virtual Machine by Using the Typical Setup	92
Create a Virtual Machine by Using the Custom Setup	94
Install a Guest Operating System Manually	96
Use a Paravirtualized Kernel in Linux Guests to Enhance Performance	98
Upgrade a Guest Operating System	99
Files That Make Up a Virtual Machine	100
Installing and Using VMware Tools	103
Components of VMware Tools	103
VMware Tools Service	104
VMware Device Drivers	104
VMware User Process	105
VMware Tools Control Panel	105
Installing VMware Tools	105
Manually Install VMware Tools in a Windows Guest Operating System	106
Configure the Video Driver on Older Versions of Windows	107
Automate the Installation of VMware Tools in a Windows Guest	108
Install VMware Tools on a Linux Guest Within X by Using the RPM Installer	110
Install VMware Tools from the Command Line with the Tar or RPM Installer	111
Install VMware Tools in a Solaris Guest	113
Install VMware Tools in a FreeBSD Guest	114
Install VMware Tools in a NetWare Virtual Machine	116
Start vmware-user Manually If You Do Not Use a Session Manager on UNIX	117

VMware Tools Update Process	117
How Automatic Updates Occur	118
How You Are Notified to Do a Manual Update	118
Use Global Settings to Update VMware Tools Automatically	119
Set Autoupdate Options for Each Virtual Machine	119
Update VMware Tools in Older Windows Virtual Machines	120
Uninstall VMware Tools	120
Repair or Change Installed Modules	120
Open the VMware Tools Control Panel	121
Use the Windows Control Panel to Display the VMware Tools Taskbar Icon	122
Options Tab Settings	122
Devices Tab Settings	124
Scripts Tab Settings	124
Shared Folders Tab Information	125
Shrink Tab Settings	125
About Tab	126
Configure VMware Tools in a NetWare Guest	126
Customizations to VMware Tools	127
How VMware Tools Scripts Affect Power States	127
Execute Commands After You Power Off or Reset a Virtual Machine	130
Passing a String from the Host to the Guest at Startup	131
Passing Information Between the Guest and Another Program	133
Use the VMware Tools Command-Line Interface	133
Options for the VMware Tools --cmd Command	135
Creating a Virtual Machine from a System Image or Another Virtual Machine	137
Conversion Process for Importing Virtual Machines from Other Formats	137
VMware Converter Compared to the Conversion Wizard in Workstation	139
Supported Source Machines	139
Operating System Compatibility	140
Importing from Various Sources	140
Supported Destinations	144
Designating a Destination for a Virtual Machine	144
Conversion Impact on Settings	146
Migration Issues Caused by Hardware Changes	147
Open a Third-Party Virtual Machine or System Image	147
Import a Virtual Machine, Virtual Appliance, or System Image	148

Getting Started with Virtual Machines	149
Starting a Virtual Machine	149
Start a Virtual Machine from the Workstation User Interface	150
Start a Virtual Machine That Is Running in the Background	150
Virtual Machine Location	151
Shut Down a Virtual Machine	152
Configure Power Off and Reset Options for a Virtual Machine	152
Delete a Virtual Machine	153
Controlling the Display	154
Using Unity Mode	154
Use Full Screen Mode	156
Report Battery Information in the Guest Operating System	158
Use Quick Switch Mode	158
Use Exclusive Mode	159
Use Multiple Monitors for One Virtual Machine	160
Use Multiple Monitors for Multiple Virtual Machines	162
Fitting the Workstation Console to the Virtual Machine Display	163
Working with Nonstandard Resolutions	165
Install New Software in a Virtual Machine	165
Disable Acceleration If a Program Does Not Run	166
Use Removable Devices in a Virtual Machine	166
Using VNC for Remote Connections to a Virtual Machine	167
Configure a Virtual Machine as a VNC Server	167
Use a VNC Client to Connect to a Virtual Machine	168
Set Up Appliance View for a Virtual Machine	169
Create a Screenshot of a Virtual Machine	171
Create and Play Back a Movie of a Virtual Machine	171
Advanced Options for Application Developers	173
Transferring Files and Text Between the Host and Guest	175
Using Drag-and-Drop	175
Enable or Disable Drag-and-Drop	176
Using Copy and Paste	176
Enable or Disable Copy and Paste	177
Using Shared Folders	177
Set Up Shared Folders	178
Enabling and Disabling Shared Folders	179
Viewing a Shared Folder	181
Permissions and Folder Mounting for Shared Folders on Linux Guests	182
Using a Mapped Drive for Windows Only	184
Map a Virtual Disk to a Drive on the Host	185

Disconnect the Host from the Virtual Disk	185
Preserving the State of a Virtual Machine	187
Using the Suspend and Resume Features	187
Use Hard Suspend or Soft Suspend	187
Suspend or Resume a Virtual Machine	188
Using Snapshots	189
Scenarios for Using Multiple Snapshots	189
Information Captured by Snapshots	191
Snapshot Conflicts	191
Enable or Disable Background Snapshots	192
Exclude a Virtual Disk from Snapshots	192
Snapshot Manager Overview	193
Take a Snapshot	195
Rename a Snapshot or Recording	196
Restore an Earlier State from a Snapshot	196
Delete a Snapshot or a Recording	197
Take or Revert to a Snapshot at Power Off	197
Snapshots and Workstation 4 Virtual Machines	198
Cloning, Moving, and Sharing Virtual Machines	199
The Virtual Machine's Universal Unique Identifier	199
UUID Options When You Move a Virtual Machine	200
Specify a UUID for a Virtual Machine	201
Cloning a Virtual Machine	201
Uses of a Clone	202
Types of Clones	202
Creating Clones	203
Moving a Virtual Machine	205
Hosts with Different Hardware	206
Move a Virtual Machine to a New Location or a New Host	207
Moving an Older Virtual Machine	209
Moving Linked Clones	209
Sharing Virtual Machines with Other Users	209
Sharing Virtual Machines with VMware Player	210
Start and Exit VMware Player	210
Setting Up Virtual Machines for Use with VMware Player	211
Using Disks and Disk Drives	213
Virtual Machine Disk Storage	213
Benefits of Using Virtual Disks	214
Physical Disks	216

Virtual Disk Maintenance Tasks	217
Defragment Virtual Disks	217
Shrink a Virtual Disk	218
Adding Virtual and Physical Disks to a Virtual Machine	219
Create a Virtual Disk and Add It to a Virtual Machine	219
Add an Existing Virtual Disk to a Virtual Machine	220
Remove a Virtual Disk from a Virtual Machine	221
Using Physical Disks in a Virtual Machine	221
Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine	227
Add DVD or CD Drives to a Virtual Machine	227
Add Floppy Drives to a Virtual Machine	229
Connect a CD-ROM, DVD, or Floppy Drive to an Image File	230
Using VMware Virtual Disk Manager	231
Using Dual-Boot Computers with Virtual Machines	231
Legacy Virtual Disks	231
 Recording and Replaying Virtual Machine Activity	 233
Uses of the Record/Replay Feature	233
Physical and Virtual Hardware Requirements	234
Enabling Record/Replay for a Virtual Machine	235
Record Control Dialog Box Features	236
Replay Control Dialog Box Features	237
Making a Recording	238
Replaying a Recording	239
Browsing a Recording	240
Creating an Execution Trace File of a Recording	240
Maintenance Tasks for Using Recordings	241
Deleting a Recording	241
Disabling Periodic Screenshots	242
Set the Debugging Mode	242
 Configuring Teams	 245
Benefits of Using Teams	245
Managing Teams	246
Create a Team	246
Open a Team and Add It to the Favorites List	247
Change the Name of a Team	248
Power Off or Close a Team	248
Delete a Team	249
Summary and Console Views for Teams and Their Virtual Machines	249

Managing the Members of a Team	251
Add a Virtual Machine to a Team	251
Remove a Virtual Machine from a Team	251
Specify the Startup Sequence for a Team	252
Power Operations for Teams and Their Members	253
Power On a Team	253
Suspend or Resume a Team	253
Perform Power Operations on One Team Member	254
Working with Team Networks	254
LAN Segment Requirements Regarding IP Addresses	254
Create a Team LAN Segment	254
Configure LAN Segments	255
Add or Remove Network Adapters	256
Delete a LAN Segment	256
Cloning and Taking Snapshots of Team Virtual Machines	257
 Configuring a Virtual Network	 259
Components of the Virtual Network	259
Virtual Switch	259
DHCP Server	260
Network Adapter	260
Common Networking Configurations	260
Bridged Networking	261
Network Address Translation (NAT)	262
Host-Only Networking	263
Example of a Custom Networking Configuration	265
Set Up a Custom Networking Configuration	265
Changing a Networking Configuration	267
Find the Network Type of a Virtual Machine	268
Add Virtual Network Adapters	268
Modify Existing Virtual Network Adapters	269
Configuring Bridged Networking	269
Configure vmnet0 Bridged Networking on a Windows Host	270
Configure vmnet0 Automatic Bridged Networking on a Linux Host	271
Changing the Subnet or DHCP Settings for a Virtual Network	272
Change Subnet or DHCP Settings on a Windows Host	272
Change Subnet or DHCP Settings on a Linux Host	274
Configuring Host Virtual Network Adapters	275
Enable or Disable a Host Virtual Adapter	276
Add or Remove a Host Virtual Adapter	276

Advanced Virtual Networking	277
Selecting IP Addresses on a Host-Only Network or NAT Configuration	277
How the Subnet Number Is Assigned	278
Determining Whether to Use DHCP or Statically Assign Addresses	278
Configuring the DHCP Server on a Linux Host	279
Configure the DHCP Server on a Windows Host	279
DHCP Conventions for Assigning IP Addresses	279
Avoiding IP Packet Leakage in a Host-Only Network	280
Packet Leakage in Virtual Machines	280
Using Filtering	280
Disable Packet Forwarding on Windows Hosts	281
Install Windows 2000 Administrative Tools on a Local Computer	281
Disable Packet Forwarding on Linux Host	282
Maintaining and Changing the MAC Address of a Virtual Machine	282
Avoiding MAC Address Changes	283
Manually Assigning a MAC Address	283
Controlling Routing Information for a Host-Only Network on Linux	284
Potential Issues with Host-Only Networking on Linux	285
DHCPD on the Linux Host Does Not Work After Installing Workstation	285
DHCP and Dynamic Domain Name Service (DDNS)	285
Set Up a Second Bridged Network Interface on a Linux Host	286
Setting Up Two Separate Host-Only Networks	286
Set up a Second Host-Only Network on a Windows Host	287
Set up a Second Host-Only Network on a Linux Host	287
Configuring the Host-Only Virtual Machines	288
Set Up Using Configuration 1 or 2	288
Set Up Using Configuration 3	289
Complete Configuring the Virtual Network Adapters	289
Set Up Routing Between Two Host-Only Networks	290
Using Virtual Network Adapters in Promiscuous Mode on a Linux Host	292
Using NAT	292
How the NAT Device Uses the vmnet8 Virtual Switch	293
DHCP on the NAT Network	293
DNS on the NAT Network	293
External Access from the NAT Network	294
Advanced NAT Configuration	295
Configure NAT on a Windows Host	295
Custom NAT and DHCP Configuration on a Windows Host	296
Specifying Connections from Ports Below 1024	297
Configuring NAT on a Linux Host	297
Considerations for Using NAT	300

Using NAT with NetLogon	301
Sample Linux nat.conf File	303
Using Samba with Workstation	305
Add Users to the Samba Password File	305
Using a Samba Server for Bridged and Host-Only Networks	305
Use Samba Without Network Access	306
 Configuring Video and Sound	 307
Setting Screen Color Depth	307
Changing Screen Color Depth on the Host	308
Changing Screen Color Depth in the Virtual Machine	308
Support for Direct3D Graphics	308
Accelerated 3-D Restrictions	308
Enabling Accelerated 3-D	309
Configuring Sound	310
Installing Sound Drivers in Windows 9x and NT Guests	311
 Connecting Devices	 313
Using Parallel Ports	313
Add a Virtual Parallel Port to a Virtual Machine	313
Drivers for Iomega Zip Drives on Windows 95 and 98 Guests	314
Configuring a Parallel Port on a Linux Host	314
Using Serial Ports	318
Add a Virtual Serial Port to a Virtual Machine	318
Connect an Application on the Host to a Virtual Machine	319
Use a Serial Port Connection Between Two Virtual Machines	320
Change the Input Speed of the Serial Connection	322
Debugging over a Virtual Serial Port	322
Configuring Keyboard Features	324
Use the Enhanced Virtual Keyboard for Windows Hosts	324
Hot Keys for Virtual Machines	325
Specify a Language Keyboard Map for VNC Clients	325
Keyboard Mapping on a Linux Host	327
Using USB Devices in a Virtual Machine	335
Enable the USB 2.0 Controller for a Virtual Machine	336
Add a USB Controller to a Virtual Machine	337
Connecting USB Devices	337
USB Driver Installation on a Windows Host	338
Replace USB 2.0 Drivers on a Windows 2000 Host	339
Access and Use a USB Device on a Linux Host	339
How Device Control Is Shared Between Host and Guest	340

Disconnecting USB Devices from a Virtual Machine	341
Use Smart Cards with Virtual Machines	342
Support for Generic SCSI Devices	343
Installing Required Adapters or Drivers for Some Windows Guests	343
Avoiding Concurrent Access on Linux Hosts	344
Add a Generic SCSI Device to a Virtual Machine	345
Troubleshoot Issues with Detecting Generic SCSI Devices	346
Use Two-Way Virtual Symmetric Multiprocessing	348
Use a Virtual Machine That Originally Had More Than Two Virtual Processors	348
Special-Purpose Configuration Options for Windows Hosts	351
Locking Out Interface Features for Windows Hosts Only	351
Set Administrative Lockout Preferences	352
Removing a Forgotten Password	352
Restricting the User Interface	352
Enable the Restricted User Interface	353
Return to a Snapshot with Restricted User Interface	353
Disable Restricted User Interface	354
Using Full-Screen Switch Mode for Windows Hosts Only	355
Create a Virtual Machine for Use in Full-Screen Switch Mode	355
Moving a Virtual Machine to a User's Computer	356
Configuring Full-Screen Switch Mode	356
Starting and Stopping Virtual Machines on a User's Computer	361
Guest ACPI S1 Sleep	365
Learning the Basics of ACE	367
Benefits of Using VMware ACE	367
Key Features of VMware ACE	368
VMware ACE Terminology	368
Network and Disk Space Requirements for the Administrative Workstation	369
Overview of Creating and Deploying ACE Packages	370
Overview of the ACE User Interface	371
Troubleshooting Users' Problems	372
Setting and Using Policies and Customizing VMware Player	373
Benefits of Using Policies	374
Set Policies for ACE Instances	374
Setting Access Control Policies	374
Create or Edit an Access Control Policy	375

Activation Settings	376
Authentication Settings	377
Create and Deploy an Authentication Script	377
Include a Power-On and Power-Off Script in the Package	378
Set a Recovery Key for Encrypted ACE Instances	380
Set Activation Limit	381
Active Directory Password Change Proxying	381
Setting Host to Guest Data Script Policies	382
Setting Expiration Policies	382
Setting Copy Protection Policies	383
Setting Resource Signing Policies	383
Setting Network Access Policies	384
Before You Begin Setting Host Policies	384
Use the Network Access Wizard to Configure Network Access	385
Guidelines for Specifying Zone Conditions	386
Using the Ruleset Editor to Configure Host and Guest Access	389
Change NAT Settings	391
Understanding the Interaction of Host and Guest Access Filters With Tunneling Protocols	392
Updating a Network Access Policy	392
Setting Removable Devices Policies	392
Setting USB Device Policies	393
Access Levels for USB Devices	393
Set an Access Policy for USB Devices	393
Setting Virtual Printer Policies	395
Setting Runtime Preferences Policies	395
Runtime Preferences Settings	395
Enhanced Virtual Keyboard Settings	396
Exit Behavior Settings	397
Pocket ACE Cache Settings	397
Setting Snapshot Policies	398
Setting Administrator Mode Policies	399
Use Administrator Mode on an ACE Instance	399
Setting Hot Fix Policies for Standalone ACE Instances	400
Setting the Policy Update Frequency for Managed ACE Instances	400
Control Which ACE Instances Run on a Host	401
Run Multiple ACE Instances on an End User's Machine	402
Writing Plug-In Policy Scripts	402
Sample Policy Scripts	403
Customizing the VMware Player Interface on Windows Hosts Only	407
Create and Specify a Skin File	407

Customizing the VMware Player Icons	408
Customizing the Title Bar Text	408
Customizing the Removable Device Display	409
Shortcut Key Values	411
Sample Skin File	412

Deploying ACE Instances 413

Edit Deployment Settings	413
Encryption Settings	414
Package Lifetime Settings	414
Instance Customization on Windows Hosts Only	415
Custom EULA Settings	422
Deployment Platform Settings	423
ACE Resources Directory	423
Review the Configuration of an ACE-Enabled Virtual Machine	424
Use Preview Mode to Test Policy and Deployment Settings	425
Creating a Package	426
Overview of Package Creation and Validation	426
Turn Off the VMware Tools Check for Test Deployments	428
Prerequisites for Using the Packaging Wizards	428
Use the New Package Wizard	430
View Package Properties and Add Notes	431
Perform an End-to-End Deployment Test	431
Deploy Packages	433

Pocket ACE 435

Portable Device Requirements	435
Policies and Deployment Settings for Pocket ACE	436
Create a Pocket ACE Package	436
Deploying the ACE Package on a Portable Device	437
Deploy a Single Pocket ACE Package to a Device	438
Deploy Multiple Pocket ACE Packages to a Device	438
Run the Pocket ACE Instance	439

Installing ACE Instances 441

Installing an ACE Package on a Windows Host	441
Install an ACE Instance on a Single Windows Host	441
Install an ACE Package Silently on Multiple Windows Hosts	442
Uninstall VMware Player or an ACE instance from a Windows Host	444
Installing an ACE Package on a Linux Host	444

Manually Install VMware Player on a Linux Host	445
Install the ACE Instance on a Single Linux Host	446
Install an ACE Package Silently on Multiple Linux Hosts	446
Uninstall VMware Player or an ACE Instance from a Linux Host	447
Start and Use an ACE Instance	447
Install an ACE Client License	448
Change the ACE Client License	449
Quit VMware Player	449
Troubleshooting Tools	450
ACE Tools: vmware-acetool Command-Line Tool	450
Respond to Hot Fix Requests	452
Troubleshooting Setup Issues	453
Workstation Command-Line Reference	455
Startup Options for Workstation and Virtual Machines	455
Using Startup Options in a Windows Shortcut	456
Command-Line Application for Operating Virtual Machines	457
Examples for vmrun	460
Using the Eclipse Integrated Virtual Debugger	463
Installation Requirements for the Eclipse Integrated Virtual Debugger	
Environment	464
Host System Requirements	465
Eclipse Requirements	466
Virtual Machine Requirements	466
Managing Virtual Machine Launch Configurations	469
Use Application Configurations to Start Applications in a Virtual Machine	469
Use Application Configurations to Attach to Applications Running in a Virtual Machine	471
Delete Configurations	472
Running and Debugging Applications in Virtual Machines	472
Start an Application Debugging Session in a Virtual Machine	472
Start an Application in a Virtual Machine Without Debugging	473
Attach the Debugger to an Application Running in a Virtual Machine	473
Using the Visual Studio Integrated Virtual Debugger	475
Configuration Options When Starting an Application in a Virtual Machine	476
Configuration Options When Attaching to a Process Running in a Virtual Machine	477
Setting Up the Visual Studio Integrated Virtual Debugger Environment	477
Microsoft Visual Studio Requirements and Recommendations	478

Host System Requirements	479
Virtual Machine Requirements and Recommendations	479
Troubleshooting Tips	483
Managing Virtual Machine Configurations	485
Create Configurations	485
Setting Configuration Properties	486
Rename Configurations	489
Remove Configurations	489
Running and Debugging Applications in Virtual Machines	489
Start a Debugging Session in a Virtual Machine	490
Start a Session Without Debugging in a Virtual Machine	490
Attach the Debugger to a Process Running in a Virtual Machine	491
Glossary	493
Index	501

BETA

Preface

This preface provides information about the *Workstation User's Manual* and links to VMware® technical support and educational resources.

This preface contains the following topics:

- [“About This Book”](#) on page 19
- [“Technical Support and Education Resources”](#) on page 20

About This Book

This manual, the *Workstation User's Manual*, provides information about installing and using VMware Workstation 6.

To view the most current version of the manual, see the VMware Web site:

http://www.vmware.com/support/pubs/ws_pubs.html

Intended Audience

This book is intended for anyone who needs to install, upgrade, or use VMware Workstation. Workstation users typically include people who do software development and testing or work with multiple operating systems or computing environments: software developers, QA engineers, trainers, salespeople who run demos, and anyone who wants to create virtual machines.

Document Feedback

If you have comments about this documentation, submit your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following sections describe the technical support resources available to you.

Self-Service Support

Use the VMware Technology Network (VMTN) for self-help tools and technical information:

- Product information – <http://www.vmware.com/products/>
- Technology information – <http://www.vmware.com/communities/content/>
- Documentation – <http://www.vmware.com/support/pubs>
- VMTN Knowledge Base – <http://kb.vmware.com>
- Discussion forums – <http://www.vmware.com/community>
- User groups – <http://www.vmware.com/communities/content/vmug/>

For more information about the VMware Technology Network, go to the VMware Communities page at:

<http://www.vmware.com/community/index.jspa>

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to <http://www.vmware.com/support/services>.

Reporting Problems

If you have problems while running VMware Workstation, please report them to the VMware support team. First, be sure to register your serial number. From the Workstation menu bar, choose **Help>VMware on the Web>Register Now!** You can then report your problems by submitting a support request at www.vmware.com/requestsupport.

The VMware support team might ask you to run a support script in order to gather the information needed to diagnose the problem. For example, if a virtual machine exits abnormally or crashes, run the support script to collect the appropriate log files and system information.

As of Workstation version 6.0.1, you can run the support script by clicking a button in the **Help>About VMware Workstation** box. You can also, as in previous releases, run the script from the command line.

To run the support script from the Workstation user interface

- 1 Start VMware Workstation.
For instructions, see “[Start Workstation on a Windows Host](#)” on page 61.
- 2 Choose **Help>About**.
- 3 In the About VMware Workstation dialog box that appears, click **Collect Support Data**.
- 4 In the confirmation box that appears, confirm that you want to collect support data.
On Windows hosts, after the script finishes running, it creates a .zip file and displays the path to the file.
On Linux hosts, the script creates a compressed .tgz file in the user’s home directory. Because the script is not run as root, the script displays messages indicating that it cannot collect some information. This is normal. If the VMware support team needs that information, a support representative will ask you to run the script from the command line as root. For instructions, see “[To run the support script on a Linux host](#)” on page 22.
- 5 Submit a support request to the VMware support team and include the data file.
The URL is www.vmware.com/requestsupport.

To run the support script on a Windows host

- 1 Open a command prompt.
- 2 Change to the VMware Workstation program directory:

```
C:
cd \Program Files\VMware\VMware Workstation
```

If you did not install the program in the default directory, use the appropriate drive letter and path in the `cd` command above.

- 3 Run the support script:

```
cscript vm-support.vbs
```

After the script runs, it displays the name of the directory where it has stored its output.

- 4 Use a file compression utility such as WinZip or PKZIP to zip the script output directory, and include the zip file with your support request.

If you are reporting a problem you encountered while installing VMware Workstation, you should also include your installation log file.

On a Windows host, the file is `VMInst.log`. It is saved in your `Temp` folder. On a Windows 2000, Windows XP, or Windows Server 2003 host, the default location is `C:\Documents and Settings\<username>\Local Settings\Temp`.

You can use the command `cd %temp%` to locate the `Local Settings` folder, which is hidden by default. To see its contents, open **My Computer**, go to **Tools>Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**.

To run the support script on a Linux host

- 1 Open a terminal window.
- 2 Run the support script as the user who is running the virtual machine:

```
vm-support
```

If you are not running the script as root, the script displays messages indicating that it cannot collect some information. This is normal. If the VMware support team needs that information, a support representative will ask you to run the script again as root.

The script creates a compressed `.tgz` file in the user's home directory.

- 3 Include that output file with your support request.

If you are reporting a problem you encountered while installing VMware Workstation, you should also include your installation log file.

VMware Education Services

VMware courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. For more information about VMware Education Services, go to <http://mylearn1.vmware.com/mgreg/index.cfm>.

BETA

Introduction and System Requirements

1

This chapter provides an introduction to Workstation and describes the system requirements for operating Workstation. This chapter contains the following topics:

- [“Product Benefits”](#) on page 24
- [“Overview of This Manual”](#) on page 25
- [“About the Host and Guest Computers”](#) on page 26
- [“Host System Requirements”](#) on page 26
- [“Virtual Machine Specifications”](#) on page 32
- [“Supported Guest Operating Systems”](#) on page 35

Product Benefits

Workstation is a desktop software that allows you to run multiple x86-compatible desktop and server operating systems simultaneously on a single PC, in fully networked, portable virtual machines—with no rebooting or hard drive partitioning required.

With Workstation, you spend less time procuring and configuring, and more time testing, deploying, teaching, or running demos. Over three million software development, quality assurance, training, sales, and IT professionals worldwide find Workstation an indispensable tool.

To streamline software development and testing:

- Develop and test multiple operating systems and applications on a single PC.
- Connect virtual machines to simulate and test multitier configurations.

- Use multiple snapshots and debugging support to facilitate testing.
- Archive test environments on file servers where they can be easily restored or shared.

To enhance productivity of IT professionals:

- Configure and test desktops and servers as virtual machines before deploying them to production.
- Test new multitier applications, application updates, and OS patches on a single PC.
- Host legacy applications within virtual machines, facilitating OS migrations and eliminating the need to port legacy applications.
- Create a virtual library of end-user configurations on a shared drive.

To facilitate computer-based training and software demos:

- Package and deploy classroom material in virtual machines.
- Allow students to experiment with multiple operating systems, applications, and tools in secure, isolated virtual machines.
- Configure virtual machines to undo all changes at shutdown.
- Demo complex or multitier configurations on a single laptop.

Overview of This Manual

If you are a veteran user of VMware products, see the Workstation Release Notes for a list of new features. For upgrade instructions, see [Chapter 3, “Upgrading Workstation and Virtual Machines,”](#) on page 51.

If you are new to VMware Workstation, the first chapters of this manual—through [Chapter 8, “Getting Started with Virtual Machines,”](#) on page 149— provide an introduction to using VMware Workstation, guide you through the key steps for installing the software, and putting it to work.

Later chapters provide in-depth reference material for getting the most out of the sophisticated features of Workstation.

About the Host and Guest Computers

The terms host and guest describe your physical and virtual machines:

- **Host** — The physical computer on which you install the VMware Workstation software is called the host computer, and its operating system is called the host operating system.
- **Guest** — The operating system running inside a virtual machine is called a guest operating system.

For definitions of these and other special terms, see “[Glossary](#)” on page 493.

Host System Requirements

Like physical computers, the virtual machines running under Workstation perform better if they have faster processors and more memory. The sections that follow, list the supported host operating systems and hardware.

PC Hardware

- Standard x86-compatible or x86-64-compatible personal computer
- 733MHz or faster CPU minimum

Compatible processors include:

- Intel — Celeron, Pentium II, Pentium III, Pentium 4, Pentium M (including computers with Centrino mobile technology), Xeon (including “Prestonia”), Core, and Core 2 processors
- AMD — Athlon, Athlon MP, Athlon XP, Athlon 64, Duron, Opteron, Turion 64, and Sempron

For additional information on processors that are not compatible, see the VMware knowledge base at

www.kb.vmware.com. Enter **967** in the **Search** menu and select **Document Id** in the **Search In** drop-down menu, **VMwareWorkstation** in the **Product** drop-down menu, and when the search results appear, click on the Choosing a Supported Processor for VMware Workstation 4 or Workstation 5 (967) link.

- Multiprocessor systems supported
- Support for 64-bit guest operating systems is available only on the following versions of these processors:
 - Revision D or later of AMD Athlon 64, Opteron, Turion 64, and Sempron

- Intel Pentium 4, Core 2, and Xeon processors with EM64T and Intel Virtualization Technology

Memory

512MB minimum (2GB is recommended).

You must have enough memory to run the host operating system, plus the memory required for each guest operating system and for applications on the host and guest. See your guest operating system and application documentation for their memory requirements.

As of version 6.5 of Workstation, the total amount of memory you can assign to all virtual machines running on a single host is unlimited. The maximum amount of memory per virtual machine is 8GB.

Display

16-bit or 32-bit display adapter is recommended.

Disk Drives

Guest operating systems can reside on physical disk partitions or in virtual disk files.

Hard Disk

- IDE and SCSI hard drives supported.
- At least 1GB free disk space recommended for each guest operating system and the application software used with it. If you use a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer.
- **For installation** – 200MB (Linux) or 900MB (Windows) free disk space required for basic installation. You can delete the installer afterwards to reclaim disk space.

Optical CD-ROM/DVD-ROM Drive

- IDE and SCSI optical drives supported.
- CD-ROM and DVD-ROM drives supported.
- ISO disk image files supported.

Floppy Drives

Virtual machines can connect to the host's floppy drives. Floppy disk image files are also supported.

Local Area Networking (Optional)

- Any Ethernet controller supported by the host operating system.
- Non-Ethernet networks supported using built-in network address translation (NAT) or using a combination of host-only networking plus routing software on the host operating system.

Host Operating System

VMware Workstation is available for both Windows and Linux host operating systems.

Windows Host Operating Systems

Workstation supports the following Windows 32-bit and 64-bit host operating systems.

Table 1-1. Windows Host Operating Systems

Processor Type	Operating System Edition
32-bit	Windows Vista Enterprise Edition
	Windows Vista Business Edition
	Windows Vista Home Basic and Premium Editions
	Windows Vista Ultimate Edition
	Windows Server 2008
	Windows Server 2003 Standard Edition, SP1, SP2
	Windows Server 2003 Web Edition, SP1
	Windows Server 2003 Small Business Edition, SP1, SP2
	Windows Server 2003 Enterprise Edition, SP1, SP2
	Windows Server 2003 R2
	Listed versions are also supported with no service pack.
	Windows XP Home Edition, SP1, SP2
	Windows XP Professional, SP1, SP2
	Windows 2000 Server SP3, SP4
	Windows 2000 Professional, SP3, SP4
	Windows 2000 Advanced Server, SP3, SP4

Table 1-1. Windows Host Operating Systems

Processor Type	Operating System Edition
64-bit	Windows Vista Enterprise Edition
	Windows Vista Business Edition
	Windows Vista Home Basic and Premium Editions
	Windows Vista Ultimate Edition
	Windows Server 2008 x64 Edition
	Windows Server 2003 x64 Edition SP1
	Windows Server 2003 x64 Edition R2 SP2
	Windows XP Professional x64 Edition

A Web browser is required for the Help system.

Linux Host Operating Systems

Workstation supports the following Linux 32-bit and 64-bit distributions and kernels for the host operating systems. Workstation might not run on systems that do not meet these requirements.

As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. VMware makes every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list below, its use with VMware products is not supported. Look for newer prebuilt modules in the download area of the VMware Web site.

Table 1-2. Linux Host Operating Systems

Processor Type	Operating System Edition
32-bit	Mandriva Linux 2006 and 2007
	Mandriva Corporate Desktop 4.0
	Mandriva Corporate Server 4.0
	Mandrake Linux 10.1
	Mandrake Linux 9.0 — stock 2.4.19
	Red Hat Enterprise Linux 5.0
	Red Hat Enterprise Linux WS 4.5 (formerly called 4.0 Update 5)
	Red Hat Enterprise Linux AS 4.0, updates 1, 2, 3, 4
	Red Hat Enterprise Linux ES 4.0, updates 1, 2, 3, 4
	Red Hat Enterprise Linux WS 4.0, updates 1, 2, 3, 4
	Red Hat Enterprise Linux AS 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8
	Red Hat Enterprise Linux ES 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8
	Red Hat Enterprise Linux WS 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8
	Red Hat Enterprise Linux 2.1 — stock 2.4.9-e3
	Red Hat Linux 9.0 — stock 2.4.20-8, upgrade 2.4.20-20.9
	Red Hat Linux 8.0 — stock 2.4.18
	Red Hat Linux 7.3 — stock 2.4.18
	Red Hat Linux 7.2 — stock 2.4.7-10, upgrade 2.4.9-7, upgrade 2.4.9-13, upgrade 2.4.9-21, upgrade 2.4.9-31
	Red Hat Linux 7.1 — stock 2.4.2-2, upgrade 2.4.3-12
	Red Hat Linux 7.0 — stock 2.2.16-22, upgrade 2.2.17-14
	SUSE Linux Enterprise Server 10 SP1
	SUSE Linux Enterprise Server 9 SP4
	SUSE Linux Enterprise Server 9, 9 SP1, 9 SP2, 9 SP3
	SUSE Linux Enterprise Server 8, stock 2.4.19
	Listed versions are also supported with no service pack.

Table 1-2. Linux Host Operating Systems

Processor Type	Operating System Edition
	openSUSE 10.3
	openSUSE 10.2 (formerly known as SUSE Linux 10.2)
	SUSE Linux 10.1
	SUSE Linux 10
	SUSE Linux 9.3
	SUSE Linux 9.2, SP1)
	SUSE Linux 9.1 — stock 2.6.4-52
	SUSE Linux 9.0 — stock 2.4.21-99
	SUSE Linux 8.2 — stock 2.4.20
	Ubuntu Linux 7.04
	Ubuntu Linux 6.10
	Ubuntu Linux 6.06
	Ubuntu Linux 5.10
	Ubuntu Linux 5.04
64-bit	Mandriva Linux 2006 and 2007
	Mandriva Corporate Desktop 4.0
	Mandriva Corporate Server 4.0
	Note: On 64-bit Mandriva hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit <code>glibc</code> , <code>X11</code> , and <code>libXtst.so</code> are required.
	Red Hat Enterprise Linux 5.0
	Red Hat Enterprise Linux 4.8
	Red Hat Enterprise Linux 4.7
	Red Hat Enterprise Linux 4.6
	Red Hat Enterprise Linux 4.5 (formerly called 4.0 Update 5)
	Red Hat Enterprise Linux AS 4.0, updates 3, 4
	Red Hat Enterprise Linux ES 4.0, updates 3, 4
	Red Hat Enterprise Linux WS 4.0, updates 3, 4
	Red Hat Enterprise Linux AS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8
	Red Hat Enterprise Linux ES 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8
	Red Hat Enterprise Linux WS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8

Table 1-2. Linux Host Operating Systems

Processor Type	Operating System Edition
64-bit	SUSE Linux Enterprise Server 10 SP1 SUSE Linux Enterprise Server 9 SP4 SUSE Linux Enterprise Server 9, SP1, SP2, SP3 Listed versions are also supported with no service pack. openSUSE 10.3 openSUSE 10.2 (formerly known as SUSE Linux 10.2) SUSE Linux 10.1 SUSE Linux 10 SUSE Linux 9.3 SUSE Linux 9.2, SP1 SUSE Linux 9.1 — stock 2.6.4-52
	Ubuntu Linux 7.04 Ubuntu Linux 6.10 Ubuntu Linux 6.06 Ubuntu Linux 5.10 Ubuntu Linux 5.04 Note: On 64-bit Ubuntu 6.x hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit <code>glibc</code> and <code>X11</code> are required.

See the *VMware Guest Operating System Installation Guide* for version details about these operating systems. A Web browser is required for the Help system.

Virtual Machine Specifications

The following sections describe the devices supported by Workstation virtual machines.

Processor

- Same processor as that on host computer.
- One virtual processor on a host with one or more logical processors.
- Two virtual processors (two-way virtual symmetric multiprocessing, or Virtual SMP™) on a host with at least two logical processors.

The following are all considered to have two logical processors:

- A multiprocessor host with two or more physical CPUs
- A single-processor host with a multicore CPU
- A single-processor host with hyperthreading enabled

See [“Use Two-Way Virtual Symmetric Multiprocessing”](#) on page 348.

Chip Set

- Intel 440BX-based motherboard
- NS338 SIO
- 82093AA IOAPIC

BIOS

PhoenixBIOS 4.0 Release 6 with VESA BIOS

Memory

Up to 8GB, depending on host memory.

No maximum limit for the total available for all virtual machines.

Graphics

VGA and SVGA support

IDE Drives

- Up to four devices—disks, CD-ROM or DVD-ROM (DVD drives can be used to read data DVD-ROM discs; DVD video is not supported).
- Hard disks can be virtual disks or physical disks.
- IDE virtual disks up to 950GB.
- CD-ROM can be a physical device or an ISO image file.

SCSI Devices

- Up to 60 devices.
- SCSI virtual disks up to 950GB.
- Hard disks can be virtual disks or physical disks.
- Generic SCSI support allows devices to be used without need for drivers in the host operating system. Works with scanners, CD-ROM, DVD-ROM, tape drives and other SCSI devices.
- LSI Logic LSI53C10xx Ultra320 SCSI I/O controller.

- Mylex (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows Server 2003).

Floppy Drives

- Up to two 1.44MB floppy devices.
- Physical drives or floppy image files.

Serial (COM) Ports

- Up to four serial (COM) ports.
- Output to serial ports, Windows or Linux files, or named pipes.

Parallel (LPT) Ports

- Up to three bidirectional parallel (LPT) ports.
- Output to parallel ports or host operating system files.

USB ports

- USB 1.1 UHCI controller, with a (transparent) virtual hub so that more than two devices can be connected.
- USB 2.0 EHCI controller that supports up to six devices. (You need use the virtual machine settings editor to enable USB 2.0 support. See [“Enable the USB 2.0 Controller for a Virtual Machine”](#) on page 336.)
- Supports most devices, including USB printers, scanners, PDAs, hard disk drives, memory card readers and digital cameras, as well as streaming devices such as webcams, speakers, and microphones.

Keyboard

104-key Windows 95/98 enhanced

Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported
- USB tablets supported

Ethernet Card

- Up to 10 virtual Ethernet cards.
- AMD PCnet-PCI II compatible.
- For 64-bit guests: Intel Pro/1000 MT Server Adapter compatible.

Sound

- Sound output and input.
- Emulates Creative Labs Sound Blaster AudioPCI. (Does not support MIDI input or game port controller/joysticks.)

Virtual Networking

- Support for 10 virtual Ethernet switches on Microsoft Windows host operating systems. Support for 255 virtual Ethernet switches on Linux hosts. Three switches are configured by default for bridged, host-only, and NAT networking.
- Support for most Ethernet-based protocols, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell Netware, and Network File System.
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP, and Telnet, including VPN support for PPTP over NAT.

Supported Guest Operating Systems

This section provides a simplified list of guest operating systems supported for virtual machines running in VMware Workstation. For the most recent list of supported guest operating systems, including detailed information about the specific operating system versions, service packs, and updates supported, see the *VMware Guest Operating System Installation Guide*, on the VMware documentation Web site. This guide also provides notes on installing the most common guest operating systems.

Operating systems that are not listed in the sections that follow are not supported for use in a Workstation virtual machine.

Table 1-3. Guest Operating Systems

Processor Type	Operating System Edition
Windows 32-bit	Windows Vista (3-D effects not yet supported)
	Windows Server 2008 (3-D effects not yet supported)
	Windows Server 2003, Small Business Server 2003
	Windows Server 2003 Web Edition
	Windows XP Professional and Home Edition
	Windows 2000 Professional
	Windows 2000 Server
	Windows 2000 Advanced Server
	Windows NT Workstation and Server 4.0
	Windows NT 4.0 Terminal Server Edition
	Windows Me
	Windows 98
	Windows 95
Windows 64-Bit	Windows for Workgroups
	Windows 3.1
	Windows Vista x64 Edition (3-D effects not yet supported)
	Windows Server 2008 x64 Edition(3-D effects not yet supported)
Microsoft MS-DOS	Windows Server 2003 x64 Edition
	Windows XP Professional x64
Microsoft MS-DOS	MS-DOS

Table 1-3. Guest Operating Systems

Processor Type	Operating System Edition
Linux 32-bit	Mandriva Linux 2006 and 2007
	Mandrake Linux
	Novell Linux Desktop
	Red Hat Linux
	Red Hat Enterprise Linux, Advanced Server, Enterprise Server, and Workstation
	SUSE Linux, openSUSE Linux
	SUSE Linux Enterprise Server, Enterprise Desktop, Desktop Server
	Sun Java Desktop System (JDS)
	Turbolinux Server, Enterprise Server, Workstation, Desktop
	Ubuntu Linux
Linux 64-Bit	Mandriva Linux 2006 and 2007
	Mandriva Linux 2006 and 2007
	Red Hat Enterprise Linux, Advanced Server, Enterprise Server, and Workstation
	SUSE Linux, openSUSE Linux
	SUSE Linux Enterprise Server, Enterprise Desktop, Desktop Server
	Turbolinux Server
	Ubuntu Linux
Novell NetWare 32-Bit	NetWare
Novell Open Enterprise Server 32-Bit	Open Enterprise Server 32-bit
FreeBSD 32-Bit	FreeBSD 32-bit Note: If you use SCSI virtual disks larger than 2GB with FreeBSD 4.0–4.3, the guest operating system does not boot. To work around this issue, see the <i>VMware Guest Operating System Installation Guide</i> .
FreeBSD 64-Bit	FreeBSD 64-bit
Sun Solaris 32-Bit	Solaris x86 32-bit
Sun Solaris 64-Bit	Solaris x86 64-bit

For details about operating systems that are newly added for this beta release, see the Workstation 6.5 release notes.

See the *VMware Guest Operating System Installation Guide* for version details about these operating systems.

Support for 64-Bit Guest Operating Systems

Workstation supports virtual machines with 64-bit guest operating systems, running on host machines with the following processors:

- Revision D or later of AMD Athlon 64, Opteron, Turion 64, and Sempron
- Intel Pentium 4 and Core 2 processors with EM64T and Intel Virtualization Technology

Workstation supports virtual machines with 64-bit guest operating systems only on host machines that have one of the supported 64-bit processors. When you power on a virtual machine with a 64-bit guest operating system, Workstation performs an internal check: if the host CPU is not a supported 64-bit processor, you cannot power on the virtual machine.

VMware also provides a standalone utility that you can use without Workstation to perform the same check and determine whether your CPU is supported for Workstation virtual machines with 64-bit guest operating systems. You can download the 64-bit processor check utility from www.vmware.com/download.

Workstation supports virtual machines with 64-bit guest operating systems only in versions 5.5 and later. If your version of Workstation is 5.0 or earlier, upgrade to version 6.0 or later for 64-bit guest operating system support. A virtual machine created in Workstation version 5.5 with a 64-bit operating system cannot be powered on or resumed in Workstation versions 5.0 and earlier.

Installing VMware Workstation

2

This chapter discusses how to install Workstation on your Linux or Windows host. This chapter contains the following topics:

- [“Installation Prerequisites”](#) on page 39
- [“Sharing a Workstation Host with Other VMware Products”](#) on page 40
- [“Install Workstation on a Windows Host”](#) on page 41
- [“Install Workstation on a Linux Host”](#) on page 45
- [“Where to Go Next”](#) on page 49

If you are upgrading rather than performing a fresh installation, see [Chapter 3](#), [“Upgrading Workstation and Virtual Machines,”](#) on page 51.

Installation Prerequisites

Installing VMware Workstation is usually a simple process of running a standard installation wizard.

Before you run the installation program, be sure you have the following:

- **Compatible host** – Verify that the computer and host operating system meet the system requirements for running Workstation. See [“Host System Requirements”](#) on page 26.
- **Workstation installation software** – If you bought the packaged distribution of Workstation, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the file you downloaded.

Workstation is available for both Windows and Linux host computers. The installation files for both host platforms are included on the same CD-ROM.

- **Workstation serial number** – Your serial number is on the registration card in your package. If you purchased Workstation online, the serial number is sent by email.

Your serial number allows you to use Workstation only on the host operating system for which you licensed the software. For example, if you have a serial number for a Windows host, you cannot run the software on a Linux host.

You need one license for each user.

To use Workstation on a different host operating system, purchase a license on the VMware Web site. You can also get an evaluation license at no charge for a 30-day evaluation of the software. For more information, go to the VMware Web site.

If you do not enter the Workstation serial number at installation time (an option available on a Windows host), you are prompted to enter it the first time you attempt to power on a virtual machine.

- **A guest operating system** – After Workstation is installed, you need the operating system installation CDs or ISO image files to set up a guest in a virtual machine.
- **(Optional) Eclipse or Microsoft Visual Studio** – To install the Eclipse or Visual Studio Integrated Virtual Debugger plug-ins included with Workstation, Eclipse or Visual Studio must be installed on the host before you run the Workstation installer. If you install one or both of these programs after you install Workstation, run the Workstation installer again and select the **Modify** option to install the plug-ins at that time.

Sharing a Workstation Host with Other VMware Products

You cannot have VMware Workstation installed on the same host machine with another VMware product, such as VMware Server or the VMware Virtual Machine Console. The only VMware products that can share a host machine with Workstation are the VMware VirtualCenter client software and VMware Converter. If you plan to install VMware Workstation on a host machine that already contains another VMware product, you must uninstall that product first.

After you complete the prerequisites and determine which computer you want to use for hosting Workstation, see the appropriate installation topic:

- [“Install Workstation on a Windows Host”](#) on page 41
- [“Install Workstation on a Linux Host”](#) on page 45

Install Workstation on a Windows Host

Before you begin, make sure you have the items listed in [“Installation Prerequisites”](#) on page 39. Although you can enter the number after installation, VMware recommends entering it at installation time.

This topic describes how to complete the interactive Workstation installation wizard. To instead use the command-line interface to perform a silent installation on many computers, see [“Install Workstation Silently”](#) on page 43.

To install Workstation on a Windows host

- 1 Log in to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

Log in as local administrator (that is, do not log on to the domain, unless your domain account is also a local administrator).

Although an administrator must install Workstation, a normal user—without administrative privileges—can run the program after it is installed.

- 2 From the **Start** menu, choose **Run**, and specify the path to either the CD-ROM drive or the downloaded installer file:

- If you are installing from a CD, enter **D:\setup.exe**, where D: is the drive letter for your CD-ROM drive.
- If you are installing from a downloaded file, browse to the directory where you saved the downloaded installer file, and run the installer.

The filename is similar to **VMware-workstation-<xxxx-xxxx>.exe**, where **<xxxx-xxxx>** is a series of numbers representing the version and build numbers.

On Windows Vista, when the User Account Control dialog box appears, prompting you for permission to run the installer, click **Continue**.

If you have an earlier version of Workstation installed on your system, the installer removes that version before installing the new version. After the uninstallation is complete, you might be prompted to restart your computer before the installer can install the new version.

- 3 When the wizard opens and finishes computing space requirements, click **Next** to dismiss the Welcome page.

- 4 On the Setup Type page, select **Typical** unless you do not want to install the applicable Workstation IDE plug-ins, or if you have Eclipse installed in a non-standard location.

Regarding the integrated virtual debuggers (IDE plug-ins), the installer does the following:

- If you have Visual Studio 2005 or Eclipse installed, the installer installs an integrated virtual debugger. If you don't want a plug-in installed, select the **Custom** setup, and select not to install that component.
- If you have Eclipse installed in a different directory than C:\Eclipse or C:\Program Files\Eclipse and you want to install the integrated virtual debugger for it, select the **Custom** setup, and select to install that component.

Do not attempt to install the Eclipse Virtual Debugger on 64-bit Windows hosts.

If you select **Custom**, you can use the **Space** button to find out how much disk space is required for each component of the installation. Click the **Help** button for a description of what each type of icon in the list means.

- 5 (Optional) On the Destination Folder page (for typical setups) or the Custom Setup page (for custom setups), if you do not want Workstation installed in the directory that is shown, click **Change** and specify the directory you want.

If you specify a directory that does not exist, the installer creates it for you.



CAUTION Do not install VMware Workstation on a network drive.

- 6 Click **Next**.

Windows and the Microsoft Installer limit the length of a path to a folder on a local drive to 255 characters. For a path to a folder on a mapped or shared drive, the limit is 240 characters. If the path exceeds this limit, an error message appears. You must select or enter a shorter path.

- 7 On the Configure Shortcuts page, deselect any shortcuts you do not want the installer to create.
- 8 On the Ready to Install the Program page, either click **Install** or click **Back** to make changes.
- 9 (Optional) After you click **Install**, on the Registration Information page, enter your name, company name, and serial number and click **Next**.

Your serial number is either on the registration card in your package or in an email from VMware if you purchased Workstation online. The user and company

information you enter here is then made available in the About box (choose **Help > About VMware Workstation**).

If you skip this step, you must enter your serial number before you can power on a virtual machine.

- 10 When the wizard displays the Installation Wizard Completed page, click **Finish**.

Some installations might require that you reboot your computer. When you restart, you don't need to log in as a user with Administrator privileges.

Install Workstation Silently

If you are installing Workstation on several Windows host computers, you can use the silent installation feature of the Microsoft Windows Installer. This feature is convenient, for example, in a large enterprise.

Before you begin, ensure that the host computer has version 2.0 or higher of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP and is available separately from Microsoft. For additional details on using the Microsoft Windows Installer, see the Microsoft Web site.

To install Workstation silently

- 1 Open a command prompt and enter the following command to silently extract the administrative installation image from the VMware Workstation installer:

```
setup.exe /a /s /v"/qn TARGETDIR=<install_temp_path>"
```

`setup.exe` is the name of the installer on the CD distribution. If you are using a downloaded installer, the filename is similar to `VMwareWorkstation-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers.

`<install_temp_path>` is the full path to the folder where you want to store the administrative installation image.

- 2 Enter the following command to run a silent installation using `msiexec` and the administrative installation image you extracted in the previous step:

```
msiexec -i "<install_temp_path>\VMware Workstation.msi"  
[INSTALLDIR="<path_to_program_directory>"] ADDLOCAL=ALL  
[REMOVE=<feature_name,feature_name>] /qn
```

Enter the command on one line. To install Workstation in a location other than the default, change the path that follows `INSTALLDIR=` to specify the location.

Use the optional `REMOVE=<property>` to skip installation of certain features. The `REMOVE=<property>` setting can take one or more of the values listed in [Table 2-1](#).

Table 2-1. Values for the REMOVE Property

Value	Description
Authd	VMware authorization service, which is used to perform tasks when you are not running Workstation as an Administrator user.
Network	Networking components, including the virtual bridge and the host adapters for host-only networking and NAT networking. Do not remove this component if you want to use NAT or DHCP.
DHCP	Virtual DHCP server.
NAT	Virtual NAT device.

If you specify more than one value, use a comma to separate the values. For example, REMOVE=Authd,NAT.

NOTE If you specify REMOVE=Network, the installer skips installation of certain networking components, including NAT and DHCP. There is no need to specify DHCP or NAT separately.

You can customize the installation further by adding any of the following installation properties to the command by using the format <property>=<value>. A value of 1 means true. A value of 0 means false. If you use the serial number property, enter the serial number with hyphens (xxxxx-xxxxx-xxxxx-xxxxx).

Table 2-2. PROPERTY Values

Property	Effect of the Property	Default
DESKTOP_SHORTCUT	Installs a shortcut on the desktop	1
DISABLE_AUTORUN	Disables CD autorun on the host	1
REMOVE_LICENSE	(Uninstall only) Removes all stored licenses at uninstall	0
SERIALNUMBER	Enters the serial number	

Uninstall Workstation from a Windows Host

Use the Windows Control Panel to uninstall Workstation. Workstation licenses, preference settings, and virtual machines are not removed, but virtual network settings are removed.

To uninstall Workstation from a Windows host

Depending on which version of Windows you have, do one of the following:

- On Windows Vista hosts, go to **Start > Control Panel > Programs > Programs and Features > Uninstall a program** and uninstall **VMware Workstation**.
- On other Windows hosts, use the Add/Remove Programs control panel and remove **VMware Workstation**.

Install Workstation on a Linux Host

Before you begin, read the following notes and make adjustments to your host system:

- Make sure you have the items listed in [“Installation Prerequisites”](#) on page 39.
- If you have a previous tar installation, delete the previous `vmware-distrib` directory before installing from a tar file again.

The location of this directory depends on where you placed it when you did the previous installation. Often it is placed in:

`/tmp/vmware-distrib`

- The real-time clock function must be compiled into your Linux kernel.
- Workstation for Linux requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module (that is, it must be set to `m` when the kernel is compiled).
- To use the Workstation Help system, you must have a Web browser installed on the host computer.

The following procedure describes an installation from a CD-ROM disc. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the `Linux` directory on the CD.

To install Workstation on a Linux host

- 1 Log on to your Linux host with the user name you plan to use when running Workstation.
- 2 In a terminal window, use the following command to become root so you can perform the initial installation steps:

`su -`
- 3 Mount the Workstation CD-ROM.
- 4 Change to the `Linux` directory on the CD.

- 5 Continue installation with the appropriate section for your desired installer:

- [“Using the tar Installer”](#) on page 46
- [“Using the RPM Installer”](#) on page 46

Using the tar Installer

You can skip the steps for copying and unpacking the archive and install directly from the `vmware-distrib` directory on the CD:

- a Copy the tar archive to a temporary directory on your hard drive (for example, `/tmp`):


```
cp VMware-<xxxx>.tar.gz /tmp
```
- b Change to this temporary directory:


```
cd /tmp
```
- c Unpack the archive:


```
tar xzpf VMware-<xxxx>.tar.gz
```
- d Change to the installation directory:


```
cd vmware-distrib
```
- e Run the installation program:


```
./vmware-install.pl
```
- f Accept the default directories for the binary files, library files, manual files, documentation files, and `init` script.
- g Enter **Yes** when prompted to run `vmware-config.pl`.
- h Respond to the prompts, as described in [“Run vmware-config.pl”](#) on page 47.

Using the RPM Installer

- a Run RPM specifying the installation file:


```
rpm -Uvh VMware-<xxxx>.rpm
```

`VMware-<xxxx>.rpm` is the installation file on the CD. In place of `<xxxx>` the filename contains numbers that correspond to the version and build.
- b Run the configuration program:


```
vmware-config.pl
```
- c Respond to the prompts, as described in [“Run vmware-config.pl”](#) on page 47.

Configuring Workstation with `vmware-config.pl`

This section describes how to use `vmware-config.pl` to configure your installation of VMware Workstation.

NOTE If you run the RPM installer, you need to run this program separately from the command line. If you install from the tar archive, the installer offers to launch the configuration program for you. Answer **Yes** when you see the prompt.

Required Configuration Changes

Configuration with `vmware-config.pl` is required in the following circumstances:

- When you install VMware Workstation the first time.
- When you upgrade your version of Workstation.
- When you upgrade your host operating system kernel. (It is not necessary to reinstall Workstation after you upgrade your kernel.)
- To reconfigure the networking options for Workstation—for example, to add or remove host-only networking.

Location of `vmware-config.pl`

The installer places `vmware-config.pl` in `/usr/bin`. If `/usr/bin` is not in your default path, run the program with the following command:

```
/usr/bin/vmware-config.pl
```

Run `vmware-config.pl`

After you run the installer to perform a fresh installation or an upgrade, you need to run `vmware-config.pl`. If you have not already done so, open a terminal window and become root before performing the following procedure.

To run `vmware-config.pl`

- 1 Use the following command to start the program if necessary:

```
vmware-config.pl
```

NOTE Workstation includes precompiled drivers for many types of Linux kernels, but not all. If you have any problems after running `vmware-config.pl`, when you attempt to launch Workstation, open a terminal window and run `vmware-config.pl` again, this time with the `--compile` option:

```
vmware-config.pl --compile
```

- 2 Respond to the prompts. In most cases, the default response is appropriate.

Take the following considerations into account:

- If you have Eclipse installed and want to install Workstation's Integrated Virtual Debugger for Eclipse, enter **Yes**, when prompted. (The default is **No**.)
- If you want to install the Integrated Virtual Debugger for Eclipse, when you are prompted to install the VIX API and accept its license agreement, do so. The debugger cannot run without the VIX API.

If the configuration program does not display a message saying the configuration completed successfully, run the configuration program again.

- 3 When done, exit from the root account:

```
exit
```

The first time you attempt to power on a virtual machine, you are prompted to enter the Workstation 6.5 serial number.

Uninstall Workstation from a Linux Host

When you uninstall Workstation, product licenses, preference settings, and virtual machines are not removed, but virtual network settings are removed.

To uninstall Workstation from a Linux host

Depending on whether you used a tar installer or an RPM installer when you installed Workstation, do one of the following:

- If you used the RPM installer, enter the following command:

```
rpm -e VMwareWorkstation<xxxx>
```

Where <xxxx> is a series of numbers representing the version and build. If you have Workstation properly installed, you can find the Workstation build number by running:

```
rpm -qa | grep VM
```

- If you used the tar installer, enter the following command:

```
vmware-uninstall.pl
```


Where to Go Next

After Workstation is installed, the process of using it usually includes the following tasks performed in the following order:

- 1 Create a virtual machine.

See [Chapter 5, “Creating a Virtual Machine,”](#) on page 85.

- 2 Install a guest operating system in the new virtual machine.

See [“Install a Guest Operating System Manually”](#) on page 96 or the *VMware Guest Operating System Installation Guide*, available from the **Help** menu.

- 3 Install the VMware Tools package in the virtual machine.

See [Chapter 6, “Installing and Using VMware Tools,”](#) on page 103.

- 4 Start using the virtual machine.

See [Chapter 4, “Learning Workstation Basics,”](#) on page 61 and [Chapter 8, “Getting Started with Virtual Machines,”](#) on page 149.

BETA

Upgrading Workstation and Virtual Machines

3

This chapter discusses how to upgrade VMware Workstation 4, 5, or 6.0.x on your Linux or Windows host system, and how to use existing virtual machines under Workstation 6.5 or upgrade them. This chapter contains the following topics:

- [“Prepare for the Upgrade”](#) on page 51
- [“Upgrade Workstation on a Windows Host”](#) on page 53
- [“Upgrade Workstation on a Linux Host”](#) on page 55
- [“Using an Older-Version Virtual Machine Without Upgrading”](#) on page 56
- [“Change the Version of the Virtual Machine”](#) on page 57

Prepare for the Upgrade

When you install a new version of Workstation, the previous version is uninstalled but the preferences you set, license files, and virtual machines are not removed. Although you do not delete virtual machines created with an earlier version of Workstation, VMware recommends that you make backup copies and power them off completely in preparation for the upgrade.

Before you begin, make sure all virtual machines are Workstation 4, 5, or 6.0.x virtual machines. Direct upgrades from a Workstation 2 or 3 virtual machine are not supported in Workstation 6.0.x and 6.5. See [“Removing Workstation 2 or 3 to Install Workstation 6.x”](#) on page 52.

To prepare for the upgrade

- 1 If a virtual machine was created with a version of Workstation earlier than Workstation 5.5 and it has a snapshot, delete the snapshot before upgrading.

See [“Delete a Snapshot or a Recording”](#) on page 197.

- 2 If any virtual machines are suspended, resume them, shut down the guest operating system, and power them off.
- 3 If any virtual machines are running in the background, start them in Workstation and power them off.

See [“Start a Virtual Machine That Is Running in the Background”](#) on page 150.

- 4 Back up the virtual machines by making backup copies of all the files in the virtual machine directories.

This includes .vmdk or .dsk files, .vmx or .cfg files, and .nvram files. Depending on your upgrade path, you might not be able to run your virtual machines under both Workstation 6.5 and your previous version of Workstation.

- 5 For upgrades from Workstation 4, 5.x, or 6.0.x, if you bridged (mapped) virtual networks to specific physical or virtual adapters, write down the settings you used.

Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve bridge settings created with Workstation 4, 5.x, or 6.0.x.

You can now use one of the following platform-specific topics to install Workstation:

- [“Upgrade Workstation on a Windows Host”](#) on page 53
- [“Upgrade Workstation on a Linux Host”](#) on page 55

Removing Workstation 2 or 3 to Install Workstation 6.x

To install Workstation 6.5 on a computer where Workstation 2 or 3 is already installed, you must uninstall the old version before installing the new one. See the Workstation 2 or 3 documentation for instructions about uninstalling.

On a Windows host, the uninstaller might ask to remove licenses from the registry. If there is any possibility that you might want to reinstall the old version, do not allow the uninstaller to remove the licenses. You can safely keep licenses for multiple VMware products on the computer at the same time.

On a Linux host, the license remains in place. You can safely leave the license where it is.

NOTE If you have Workstation version 2 or 3 virtual machines that you want to use with Workstation 6.5, upgrade the virtual machines to at least Workstation 4 before you install Workstation 6.5.

After you uninstall the old version, you can install Workstation 6.5, as described in the following topics:

- [“Install Workstation on a Windows Host”](#) on page 41
- [“Install Workstation on a Linux Host”](#) on page 45

Upgrade Workstation on a Windows Host

You can upgrade from Workstation version 4, 5, or 6.0.x to Workstation 6.5 by running the VMware Workstation 6.5 installation program.

Before you begin, make sure that you have a Workstation 6.5 serial number. Also perform the tasks described in [“Prepare for the Upgrade”](#) on page 51.

To upgrade Workstation and upgrade the host operating system to Windows Vista, see [“Upgrading to a Windows Vista Host”](#) on page 54.

To upgrade Workstation on a Windows host

- 1 Log in to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.
- 2 Launch the Workstation 6.5 installer from your download directory or CD-ROM.

Workstation automatically uninstalls the previous version but saves all the network settings except for bridged settings used to map individual virtual networks to specific physical or virtual adapters.

- 3 Reboot your computer if you are prompted to do so, and log in again as the Administrator user or as a user who is a member of the Windows Administrators group.
- 4 Complete the installation wizard.

For detailed instructions on running the installer, see [“Install Workstation on a Windows Host”](#) on page 41.

- 5 Reboot your computer if you are prompted to do so.

You can now log in as you normally do. You do not need to log in as an Administrator now that Workstation is installed.

- 6 If you used bridged settings to map virtual networks to specific physical or virtual adapters, re-create the mappings.

Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve mappings created with Workstation 4, 5.x, or 6.0.x.

To use Workstation 6.5 to upgrade virtual machines, see [“Change the Version of the Virtual Machine”](#) on page 57.

Upgrading to a Windows Vista Host

This topic provides instructions for various upgrade scenarios that involve Windows Vista.

During the upgrade from Windows XP to Windows Vista, the location of virtual machines might get changed. The Windows Vista upgrade uses the registry to map the virtual machines to a new location by using the following paths:

- On Windows XP, the default virtual machine location before the upgrade is
C:\Documents and Settings\<user>\My Virtual Machines
- On Windows Vista, the default virtual machine location after the upgrade is
C:\Users\<user>\Documents\My Virtual Machines

After the upgrade is complete, if the **Favorites** list in Workstation does not work correctly, you can remove the virtual machines from it and add them again.

Upgrade Workstation 5 on Windows XP to Workstation 6.5 on Windows Vista

As part of the upgrade, you must uninstall the Workstation 5 application, but you do not need to uninstall Workstation 5 virtual machines.

To upgrade Workstation 5 on Windows XP to Workstation 6.5 on Windows Vista

- 1 On the Windows XP host, use the Control Panel's **Add/Remove Programs** item to uninstall Workstation 5.x.
 - 2 Upgrade the operating system to Windows Vista.
 - 3 Install Workstation 6.5.
- See [“Install Workstation on a Windows Host”](#) on page 41.
- 4 (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.

See [“Change the Version of the Virtual Machine”](#) on page 57.

Upgrade Workstation 5 on Windows Vista to Workstation 6.5 on Windows Vista

Because Workstation 5 was only experimentally supported on Windows Vista, VMware recommends manually uninstalling Workstation 5.x before installing Workstation 6.5.

As part of the upgrade, you must uninstall the Workstation 5 application, but you do not need to uninstall Workstation 5 virtual machines.

To upgrade Workstation 5 on Windows Vista to Workstation 6.5 on Windows Vista

- 1 Go to **Start > Control Panel > Programs > Programs and Features > Uninstall a program**.
- 2 Select **VMware Workstation** and click **Uninstall**.
- 3 Install Workstation 6.5.
See [“Install Workstation on a Windows Host”](#) on page 41.
- 4 (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.
See [“Change the Version of the Virtual Machine”](#) on page 57.

Upgrade Workstation 6.x on Windows XP to Workstation 6.5 on Windows Vista

Before you begin, make sure that you have Windows XP with Service Pack 2.

To upgrade Workstation 6.x from Windows XP to Windows Vista

- 1 Log in as the Administrator user or as a user who is a member of the Windows Administrators group.
- 2 Make sure that Workstation is not running and that no virtual machines are running in the background.
- 3 Upgrade the host operating system to Windows Vista, as described in the Microsoft documentation.
- 4 Run the Workstation 6.5 installer.
For more information, see [“Upgrade Workstation on a Windows Host”](#) on page 53.
- 5 (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.
See [“Change the Version of the Virtual Machine”](#) on page 57.

Upgrade Workstation on a Linux Host

You can upgrade from Workstation version 4, 5, or 6.0.x to version 6.5 by running the VMware Workstation 6.5 installation program.

Before you begin, make sure that you have a Workstation 6.5 serial number. You are prompted to enter the serial number after installation is complete, the first time you

start Workstation after the upgrade. Also perform the tasks described in [“Prepare for the Upgrade”](#) on page 51.

NOTE Starting with Workstation 5, Samba is no longer automatically configured when you run `vmware-config.pl`.

To upgrade Workstation on a Linux host

- 1 Determine whether you must uninstall the previous version of Workstation.

If you used the tar installer to install Workstation 4, 5, or 6.0.x and you use the tar installer for version 6.5, you do not need to uninstall the older version. Similarly, if you used the RPM installer to install version 4, 5, or 6.0.x and you use the RPM installer for version 6.5, you do not need to uninstall the older version.

If you manually uninstall the older version, Workstation cannot save the network settings. If you install the new version over the older version, Workstation 6.5 saves network settings except for bridged settings used to map individual virtual networks to specific physical or virtual adapters.

To manually uninstall Workstation, see [“Uninstall Workstation from a Linux Host”](#) on page 48.

- 2 Run the Workstation installer as you would for a new installation.

See [“Install Workstation on a Linux Host”](#) on page 45.

- 3 If you used bridged settings to map virtual networks to specific physical or virtual adapters, re-create the mappings.

Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve mappings created with Workstation 4, 5.x, or 6.0.x.

To use Workstation 6.5 to upgrade virtual machines, see [“Change the Version of the Virtual Machine”](#) on page 57.

Using an Older-Version Virtual Machine Without Upgrading

You might not want to upgrade a virtual machine because you want it to remain compatible with other VMware products you are using. Following is a brief summary of VMware product version compatibility:

- A virtual machine created in Workstation 4.x is compatible with GSX Server 3.x, VMware Server 1.x and 2.x, ESX Server 2.x, VMware Fusion 1.1, and ACE 1.x and 2.x.

- A virtual machine created in Workstation 5.x is compatible with VMware Server 1.x and 2.x, ESX Server 3.x, VMware ACE 2.x, and VMware Player 1.x and 2.x.
- A virtual machine created in Workstation 6.0.x is compatible with VMware Server 2.x, VMware Fusion 1.1, VMware ACE 2.x, and VMware Player 2.x.

You can run these virtual machines in Workstation 6.5, but you will not have the benefits of the new features of Workstation 6.5.

For more information about compatibility between VMware products, refer to the *VMware Virtual Machine Mobility Planning Guide*.

If you decide not to upgrade a virtual machine, you still need to upgrade VMware Tools to the new version. Follow the instructions for your guest operating system in [“VMware Tools Update Process”](#) on page 117. Do not remove the older version of VMware Tools before installing the new version.

Change the Version of the Virtual Machine

If you created virtual machines with an earlier version of Workstation, you must upgrade to the latest version to use the newest features. For information about new features, see the release notes.

If, however, you created Workstation 6.5 virtual machines but you now want to deploy those virtual machines to run on a different VMware product, you might need to downgrade to a version that is compatible with that product.

The Change Version wizard enables you to do either of these tasks.

Using Workstation 6.5, you have the following upgrade and downgrade choices:

- Upgrade a Workstation 4 virtual machine to Workstation 5, 6.0.x, or 6.5.
- Upgrade a Workstation 5 virtual machine to version 6.0.x or 6.5 or downgrade it to version 4.
- Downgrade a Workstation 6.x virtual machine to either version 4 or version 5.

The Change Version wizard also helps you determine which virtual hardware version to use.

Consider the following when changing the virtual hardware version of a virtual machine:

- The wizard lets you either change the version of the original virtual machine or create a full clone, so that the original remains unaltered.

- If you upgrade a Workstation 4 or 5 virtual machine that is compatible with ESX Server to Workstation 6.x, you will not be able to later downgrade it again to an ESX-compatible virtual machine by using the Change Version wizard.

On Windows hosts, you can, however use the Converter Import wizard (choose **File > Import**) to perform such a downgrade.

- When you upgrade a Windows XP, Windows Server 2003, or Windows Vista virtual machine, the Microsoft product activation feature might require you to reactivate the guest operating system.

To change the virtual hardware version of a virtual machine

- 1 Make backup copies of the virtual disks (.vmdk files).
- 2 In the guest operating system, make a note of the NIC settings.

Specifically, if you specified a static IP address for this virtual machine, after the upgrade, that setting could get changed to automatic assignment by DHCP.

To check the NIC settings, use the method appropriate for your operating system. For example, on Windows XP, you can use the Control Panel's Network Connections item to find information about the TCP/IP address for the virtual machine.
- 3 Shut down the guest operating system and power off the virtual machine.
- 4 Select the virtual machine and choose **VM > Upgrade or Change Version**.
- 5 Complete the pages of the Change Version wizard.

When you select a hardware compatibility version, you see a list of the VMware products that are compatible with that version. If you select Workstation 4, 5, or 6.0.x you also see a list of Workstation 6.5 features that are not supported for that version.
- 6 Power on the virtual machine.

If you upgrade a virtual machine that contains a Windows 98 operating system to a Workstation 6.5 virtual machine, you are prompted to install a PCI-PCI bridge driver when you power on the virtual machine. Because Workstation 6.5 has 32 more PCI-PCI bridges than Workstation 6.0.x, you might need to respond to the prompt 32 or 33 times.
- 7 In the guest operating system, check the NIC settings and adjust them if they changed, as described in [Step 2](#).
- 8 If the virtual machine does not have the latest version of VMware Tools installed, update VMware Tools.

Even if, for example, you upgraded a Workstation 4 virtual machine to Workstation 5 rather than 6.5, you should still update VMware Tools to the version included with Workstation 6.5. See [“VMware Tools Update Process”](#) on page 117. Do not remove the older version of VMware Tools before installing the new version.

If you are upgrading a virtual machine that runs from a physical (raw) disk, you can safely ignore the message: “Unable to upgrade <drivename>. One of the supplied parameters is invalid.” Click **OK** to continue the upgrade.

BETA

BETA

Learning Workstation Basics

4

This chapter discusses launching the Workstation program and introduces the VMware Workstation window. This chapter includes the following topics:

- [“Start Workstation on a Windows Host”](#) on page 61
- [“Start Workstation on a Linux Host”](#) on page 62
- [“Overview of the Workstation Window”](#) on page 62
- [“Check for Product Updates”](#) on page 74
- [“Quickly Create a Virtual Machine”](#) on page 75
- [“Introduction to Workstation Preferences”](#) on page 76
- [“Introduction to Virtual Machine Settings”](#) on page 79
- [“Closing Virtual Machines and Exiting Workstation”](#) on page 81
- [“Keyboard Shortcuts”](#) on page 82

Start Workstation on a Windows Host

Depending on the options you selected during installation, you might have a desktop shortcut, a **Start** menu item, or both for launching Workstation.

To start Workstation on a Windows host

- 1 From the **Start** menu, choose **Start > Programs > VMware > VMware Workstation**.
- 2 If this is the first time you are launching Workstation, read and accept the end user license agreement (EULA).

Start Workstation on a Linux Host

Whether you can start Workstation from a Linux GUI depends on the Linux distribution. For example, on Red Hat Enterprise Linux 5.1, the **VMware Workstation** menu item is in the **Applications > System Tools** menu.

You can always start Workstation from the command line. Although you must become root to install Workstation, you can start and run Workstation as a regular user.

To start Workstation on a Linux host

- 1 Open a terminal window.
- 2 Enter one of the following commands:
 - If `/usr/bin` is in your default path, enter the following command:
`vmware &`
 - If `/usr/bin` is not in your default path, enter the following command:
`/usr/bin/vmware &`
- 3 Read and accept the end user license agreement (EULA).

Workstation includes precompiled drivers for many types of Linux kernels, but not all. If it does not include precompiled drivers for your kernel, you are prompted to build the kernel. If you then receive an error message, open a terminal window and run the following command:

```
vmware-config.pl --copile
```

Overview of the Workstation Window

A Workstation virtual machine is like a separate computer that runs in a window on your physical computer. However, Workstation displays more than the screen of another computer. From the Workstation window, you can access and run virtual machines and teams of virtual machines. You can also switch easily from one to another.

Figure 4-1. VMware Workstation Window

The VMware Workstation window contains the following sections:

- **Home page, summary, console, or appliance view** – This main part of the window shows the virtual machines.
- **Tabs** – Each open virtual machine has its own tab. Click a tab to make that virtual machine active. Click the X to close the tab. Depending on how you configure Workstation, the virtual machine is then either powered off or continues to run in the background.
- **Sidebar** – Bookmark your favorite virtual machines and teams of virtual machines for quick access. You can also see which virtual machines are powered on. Right-click context menus enable you to perform many operations on a selected virtual machine. An additional section of the sidebar displays ACE Management Servers.
- **Status bar** – This area displays Workstation messages and an icon for each removable device. You can click or right-click an icon to disconnect it or edit its configuration.
- **Message log**— A note icon indicates whether any unread messages are present in the message log for the selected virtual machine. If the icon is dimmed, all messages have been read. To open the message log, right-click the icon and choose **Open Message Log**. Alternatively, from the menu bar, choose **VM > Message Log**.

Messages include warning information about the virtual machine, such as “Could not connect to the floppy drive” or “No bootable device was detected.” Select an item in the message log to see a longer description of the message.

Home Page and Views

Workstation displays one of four views in the main part of the window: the home page, the summary view, the console view, or the appliance view.

Home Page

Click the **Home** tab to display the Workstation home page. Use the icons on the home page to start creating a new virtual machine or open an existing virtual machine.

To close the home page, click the X to the right of the tabs on a Windows host or the X on the tab on a Linux host. To display the home page again, choose **View > Go to Home Tab**.

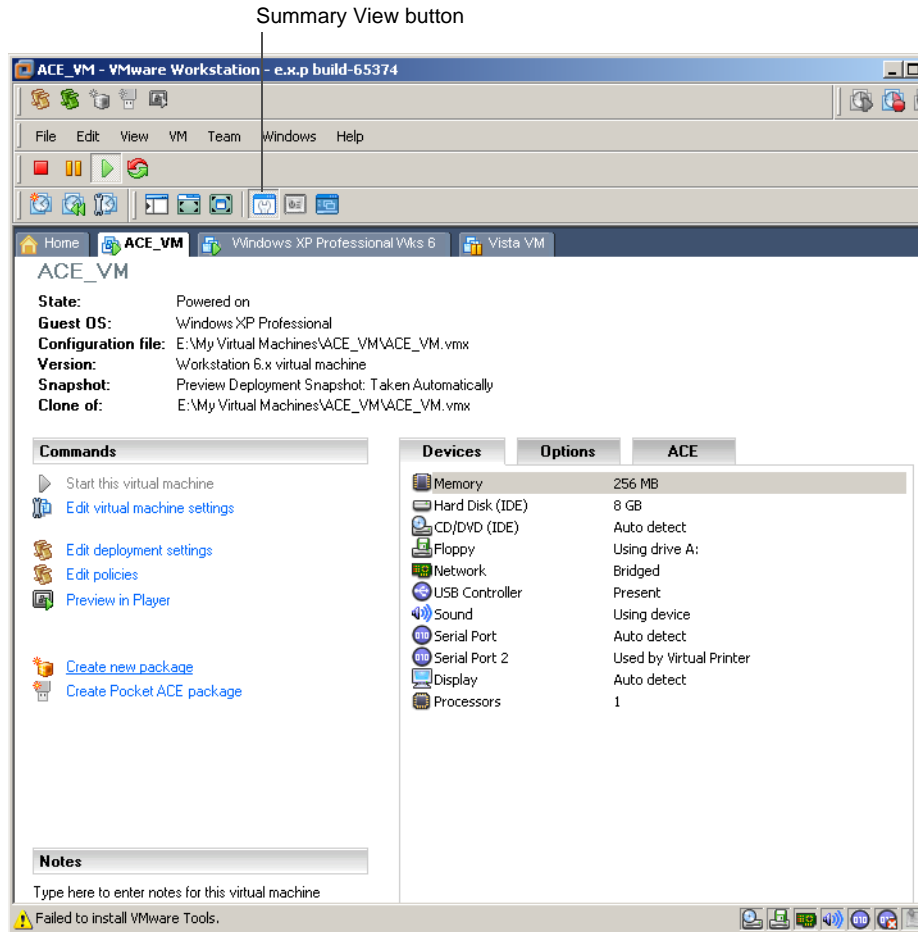
Summary View

When you select a tab for a powered-off virtual machine or team of machines, Workstation displays only a summary of the configuration information about that item. Workstation also displays a summary for a suspended virtual machine or team. Click the **Summary** toolbar button at any time to examine settings in the summary view.

Summary views appear only for virtual machines that are currently open. See [“Starting a Virtual Machine”](#) on page 149. The summary or console view remains visible as long as the virtual machine remains open.

Figure 4-2 shows an example of the summary view.

Figure 4-2. Summary View for a Virtual Machine (Windows Host)



For your convenience, the **Commands** section gives you access to the most-often used commands from the **VM** menu. On Windows hosts, for ACE-enabled virtual machines, this includes commands for creating security policies and virtual machine packages to deploy to end users, as well as a command for previewing the ACE-enabled virtual machine in VMware Player.

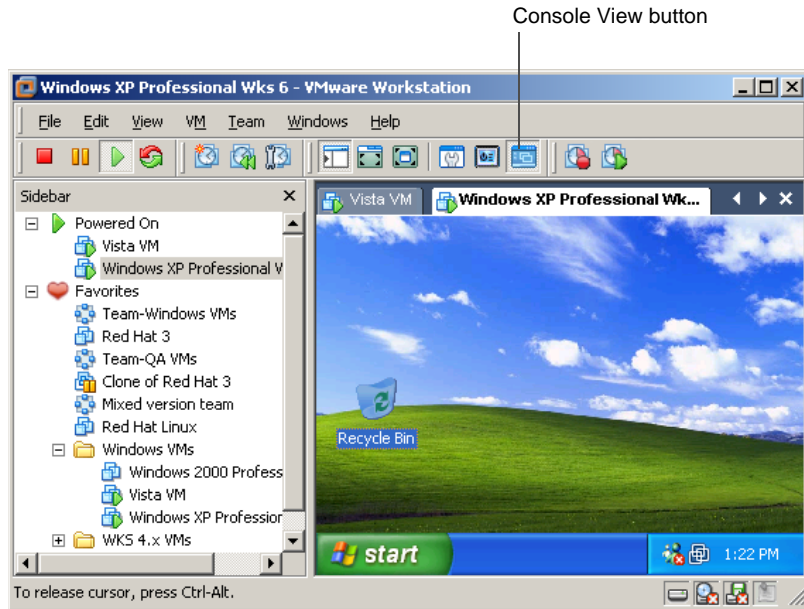
The section that includes the **Devices**, **Options**, and (sometimes) **ACE** tabs enables you to review configuration settings quickly. Double-click an item on the **Devices** or **Options** tab to display the item's configuration panel and change a setting.

For ACE-enabled virtual machines, a **Package History** section appears at the bottom of the summary view. You might need to scroll to see this section. Notes that you added to the package when creating it are displayed in the list.

Console View

The console view for an active virtual machine is like the monitor display of a physical computer.

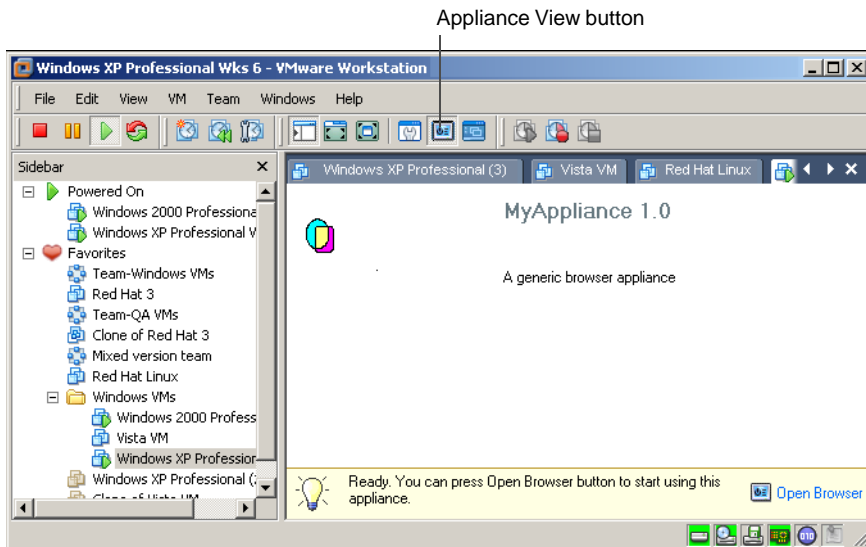
Figure 4-3. Console View (Windows Host)



When a virtual machine is active, the name of the virtual machine or team of virtual machines is displayed in a tab at the top of the console. To switch from the active virtual machine or team, click the tab of another virtual machine or team. You can use the console tabs in the windowed mode and also in the quick switch mode.

Appliance View

If you set up the virtual machine to act as an “appliance,” such as a Web server with a browser-based console, you can specify that the default view is an appliance view. The appliance view gives you a brief description of the type of server or appliance. It also provides a link that opens the browser on the host system and connects to the appliance’s management console.

Figure 4-4. Appliance View (Windows Host)

The appliance view is available only for virtual machines that you designate as appliances. See [“Set Up Appliance View for a Virtual Machine”](#) on page 169.

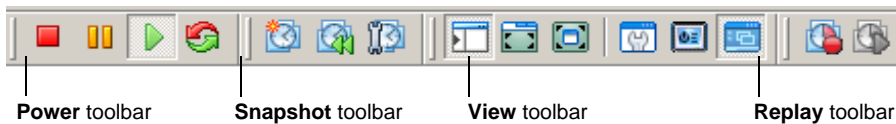
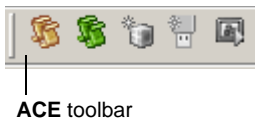
Displaying Multiple Virtual Machines at the Same Time

To simultaneously view more than one virtual machine when they are not all on the same team, open multiple Workstation windows and launch one or more virtual machines in each Workstation window.

Use a team to coordinate and use multiple virtual machines within a single console window. See [“Summary and Console Views for Teams and Their Virtual Machines”](#) on page 249.

Toolbar Buttons

The toolbar area at the top of the VMware Workstation window contains buttons you can click to power your virtual machines on and off, change the Workstation display, manage snapshots, and record virtual machine activity.

Figure 4-5. Workstation Toolbars**Figure 4-6.** ACE Toolbar (Windows Hosts Only)

If you point your mouse over a toolbar button, a tooltip appears and displays the name of the button. To change which buttons are displayed, see [“Customize the Toolbar on a Linux Host”](#) on page 70.

You can display the following toolbars:

- **Power toolbar**
 - **Power Off** – Turns off the active virtual machine or team like the power button on a physical PC. You can configure Workstation for a soft power off (called shut down) or a hard power off (called power off). See [“Shut Down a Virtual Machine”](#) on page 152 or [“Power Off or Close a Team”](#) on page 248.
 - **Suspend** – Stops a virtual machine or team in a manner that allows you to resume your work later. See [“Using the Suspend and Resume Features”](#) on page 187.
 - **Power On or Resume** – Powers on a selected virtual machine or team that is powered off, or resumes a virtual machine or team that is suspended.
 - **Power On** – See [“Starting a Virtual Machine”](#) on page 149, or [“Power On a Team”](#) on page 253.
 - **Resume** – See [“Using the Suspend and Resume Features”](#) on page 187.
 - **Reset** – Resets a virtual machine or team like the reset button on a physical PC. See [“Configure Power Off and Reset Options for a Virtual Machine”](#) on page 152.



CAUTION When a team is active, clicking the **Power On**, **Power Off**, **Suspend**, **Resume**, or **Reset** button affects all the virtual machines in that team.

- **Snapshot toolbar**

- **Take Snapshot** – Allows you to save the state of a virtual machine in the same manner you might save a word-processing document. You can come back to that state if you make a mistake by using the **Revert** button. See [“Using Snapshots”](#) on page 189.
- **Revert** – Allows you to return a virtual machine to the parent state, a state previously preserved by taking a snapshot. See [“Using Snapshots”](#) on page 189.
- **Manage Snapshots** – Opens the snapshot manager, where you can view the virtual machine’s existing snapshots, revert to a snapshot, take a new snapshot, and make a clone from a snapshot. See [“Snapshot Manager Overview”](#) on page 193.
- **View toolbar**
 - **Show or Hide Sidebar** – Toggles between showing and hiding the sidebar. See [“View the Sidebar”](#) on page 72.
 - **Quick Switch** – Enlarges the Workstation console to cover the entire host monitor. Console tabs are visible, allowing you to switch between virtual machines and teams with a single click. See [“Use Quick Switch Mode”](#) on page 158.
 - **Full Screen** – Enlarges the virtual machine display to cover the entire host monitor. The virtual machine no longer appears in a window. See [“Use Full Screen Mode”](#) on page 156.

NOTE Workstation menus and toolbars are not visible in full screen mode. Move your cursor to the top of the screen to show the full screen toolbar. Press Ctrl+Alt+Enter to restore the Workstation window.

- **Summary View** – Displays the summary view. See [“Summary View”](#) on page 64.
- **Appliance View** – Displays the appliance view. See [“Appliance View”](#) on page 66.
- **Console View** – Displays the console view. See [“Console View”](#) on page 66.
- **Replay toolbar**
 - **Replay Last Recording** – Plays the last recording made for this virtual machine.
 - **Record** – Begins recording the activity of this virtual machine.

For information about the experimental record/replay feature, see [Chapter 13, “Recording and Replaying Virtual Machine Activity,”](#) on page 233.

- **ACE toolbar** (available on Windows hosts only)
 - **Edit Policies** – Opens the policy editor.
 - **Edit Deployment Settings** – Opens the deployment settings editor.
 - **Create New Package** – Opens the New Package wizard.
 - **Create Pocket ACE Package** – Opens the Pocket ACE Package wizard.
 - **Preview in Player** – Allows you to run an ACE instance as it will run on the user's machine. Using preview mode also allows you to view the effects of changed policies as they will appear on the user's machine.

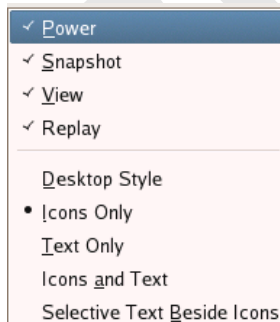
See [Chapter 20, “Learning the Basics of ACE,”](#) on page 367.

Customize the Toolbar on a Linux Host

You can customize the Workstation toolbar by adding, removing, and rearranging toolbar buttons. On a Linux host, all the buttons are contained in a single toolbar.

To customize the toolbar on a Linux host

- 1 Right-click the far-right side of the toolbar to display a **Toolbar** menu.



- 2 Choose **Power**, **Snapshot**, **View**, or **Replay** to add or remove the corresponding toolbar buttons.

When a choice is checked, the corresponding buttons are displayed.

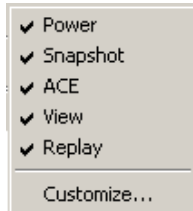
- 3 In the lower part of the menu, choose the display style for toolbar buttons.

Customize the Toolbar on a Windows Host

You can customize the Workstation toolbar by adding, removing, and rearranging toolbar buttons. On a Windows host, the toolbar buttons are arranged in separate toolbars for power buttons, snapshot buttons, view buttons, and record/replay buttons.

To customize the toolbar on a Windows host

- 1 Right-click any part of the toolbar to display a **Toolbar** menu.



- 2 Click **Power**, **Snapshot**, **ACE**, **View**, or **Replay** to add or remove that toolbar.

When a toolbar is checked, it is displayed.

To change which buttons appear in a toolbar or the order in which they appear, display that toolbar and continue with the following steps.

- 3 Right-click the **Power**, **Snapshot**, **ACE**, **View**, or **Replay** toolbar to open the Customize Toolbar window.

The Customize Toolbar window for that toolbar appears. Buttons listed under **Current Toolbar Buttons** are displayed in the toolbar, in the order shown in the Customize Toolbars window.

- 4 Make any of the following changes:

- To add or remove a button from the toolbar, select the button and click **Add** or **Remove**. Add a separator to display a vertical line between the buttons.
- To change the order of the buttons, select any button under **Current Toolbar Buttons** and click **Move Up** or **Move Down** to rearrange the buttons.
- To change the order of the currently displayed buttons without opening the Customize Toolbar window: Hold down the Shift key while you drag and drop a button to a different location in the toolbar.
- To restore the default setup, with all buttons displayed, click **Reset**.

- 5 Click **Close**.

View the Sidebar

The sidebar contains a list of favorites and shows which virtual machines or teams of virtual machines are currently powered on. On Windows hosts, an additional section of the sidebar displays ACE Management Servers. (For a description of this product, see the *VMware ACE Management Server User's Manual*.)

To view the Sidebar

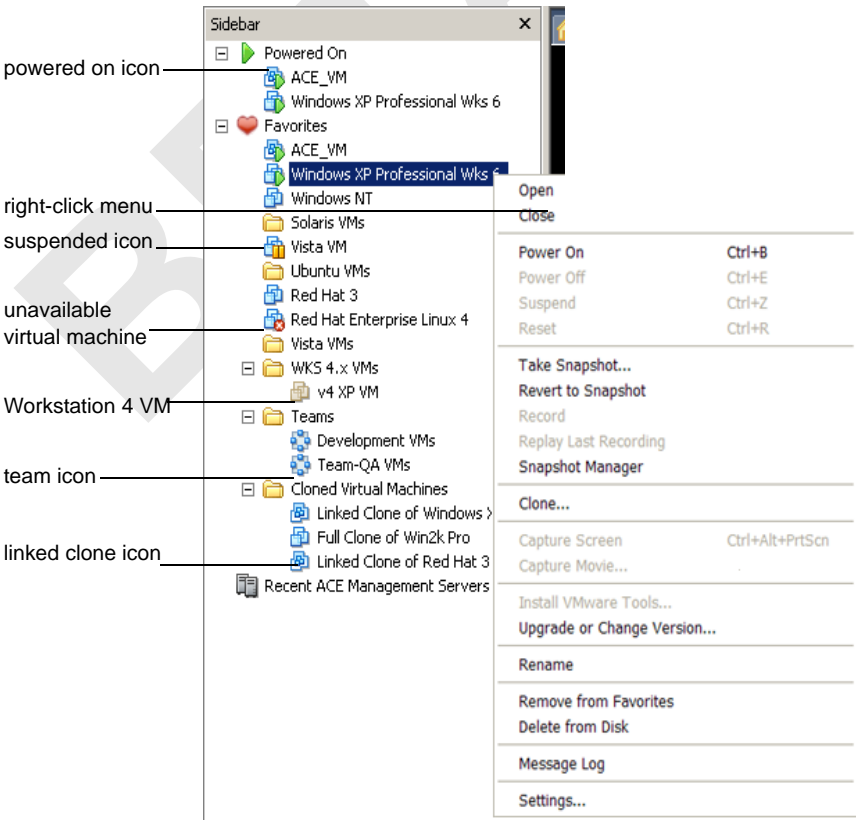
Choose **View > Sidebar**.

If the sidebar was hidden, it becomes visible. If it was visible, it is hidden.

Favorites List in the Sidebar

The **Favorites** list lets you organize and access frequently used items.

Figure 4-7. Favorites List in the Sidebar



The **Favorites** list provides the following benefits:

- **Fast access** – Quickly access frequently used items. With your virtual machines and teams on the **Favorites** list, you can open them without browsing the host file system. Also like browser bookmarks, **Favorites** list icons can be organized in folders, added, rearranged, or deleted.
- **Status** – Different icons indicate the status of virtual machines and teams. A **Favorites** list icon indicates whether the team or virtual machine is powered off, powered on, or suspended. A brown (rather than blue) virtual machine icon indicates that the virtual machine is a Workstation 4 virtual machine.
- **Right-click commands** – Right-click on a **Favorites** icon to display a menu of commands you can use for that virtual machine or team. You can click elsewhere in the **Favorites** list (that is, not on a virtual machine or team) to display a context menu from which you can choose to create a new virtual machine, team, or folder. You can also open an existing virtual machine, team, Microsoft Virtual PC or Virtual Server virtual machine, StorageCraft, or Symantec Backup Exec System Recovery system image.

Use Folders for Organizing Favorites

You can organize favorites into folders and nest folders inside other folders.

To use folders for organizing favorites

- 1 Right-click **Favorites** (or any item in the **Favorites** list), and choose **New Folder**.
- 2 Complete the New Folder dialog box that appears.
- 3 (Optional) Drag and drop folders to place one inside another.
- 4 Drag and drop Favorites items in the desired folder.

Add Virtual Machines and Teams to the Favorites List

Virtual machines and teams are automatically added to the Favorites list when you complete the New Virtual Machine wizard. You can also add them manually.

To add virtual machines and teams to the Favorites list

- 1 Choose **File > Open** and browse to the location of the virtual machine (.vmx file) or team (.vmtm file).
- 2 Click **Open**.
- 3 Choose **File > Add to Favorites**.

Remove an Item from the Favorites List

You can remove the name of a virtual machine or team from the **Favorites** list regardless of whether the virtual machine or team is open or powered on. Removing the name does not affect the virtual machine's files or operation.

To remove an item from the Favorites list

- 1 Click a name in the **Favorites** list to select it.
- 2 Choose **File > Remove from Favorites**.

Rename an Item in the Favorites List

Renaming an item in the **Favorites** list also renames the virtual machine or team.

To rename a Favorite list entry for a virtual machine or a team

- 1 Right-click the Favorites item you want to rename.
- 2 Choose **Rename** from the context menu.
- 3 Type the new name for the item and press Enter.

Powered On List

This list in the sidebar enables you to find out which virtual machines or teams are currently powered on. Right-click items in the **Powered On** list to display a menu of commands you can use for that virtual machine or team.

Check for Product Updates

Workstation automatically checks for product updates every three days. If an update check fails on two consecutive attempts, you receive a notification.

NOTE Checking for product updates works only if the host computer is connected to the Internet.

To check for product updates

- 1 (Optional) To check for updates immediately, choose **Help > Check for Updates on the Web**.
- 2 To configure Workstation to periodically check for updates, choose **Edit > Preferences > Workspace**.
- 3 In the **Software Updates** section, select the check box called **Check for software updates** and click **OK**.

Quickly Create a Virtual Machine

The instructions in this section get you started quickly with creating a virtual machine and installing a guest operating system. After you create a virtual machine, you will find the information in the rest of this chapter easier to understand.

The instructions tell you to accept the default settings so that you can complete the New Virtual Machine wizard quickly. Completing the procedure is like completing a tutorial. Later, when you want to create virtual machines that you actually use in your work or production environment, you can gain a deeper understanding of all the options available. This detailed information is provided in [Chapter 5, “Creating a Virtual Machine,”](#) on page 85.

For simplicity, use a Windows installation CD or ISO image file for the operating system you install in the virtual machine. Most Windows operating systems fit on one CD-ROM, whereas Linux requires multiple CDs.

To quickly create a virtual machine

- 1 If you plan to use an installation CD or DVD for the Windows operating system, rather than an ISO image file, insert the CD or DVD in the host CD-ROM drive.
- 2 Start VMware Workstation.
For instructions, see [“Start Workstation on a Windows Host”](#) on page 61.
- 3 Choose **File > New > Virtual Machine**.
- 4 On the Welcome page of the New Virtual Machine wizard, click **Next**.
- 5 In the Select the Appropriate Configuration page, select **Typical** and click **Next**.
- 6 On the Guest Operating system Installation page, select **Installer disc or Installer disc image file**, as appropriate, and click **Next**.

- 7 On the Easy Install Information page, specify which disk drive or ISO image file to use, the product key, and a name registering the operating system.

Specifying a password is optional. On Windows, the password you enter here is used for an account with Administrator permissions. On Windows 2000, the password is used for the Administrator account.

- 8 Click **Next**.
- 9 Complete the rest of the wizard pages as follows:
 - Name the Virtual Machine page – Click **Next** to accept the default.

- Network Type page – Select NAT and click **Next**. For Windows guests, it is recommended that you use NAT until you install security software, such as antivirus software.
- Specify Disk Capacity page – Click **Finish**.

The virtual machine is created and its name is added to the **Favorites** list.

- 10 In the Workstation window, on the tab for the newly created virtual machine, in the **Commands** section, click **Start this virtual machine**.

On Linux hosts, the command is called **Power on this virtual machine**.

The console view for the virtual machine appears. Soon the boot device (such as the CD-ROM) is detected and installation of the operating system begins.

On Windows 2000 guests, if you entered a password when completing the New Virtual Machine wizard, then when the operating system starts up, it might prompt you to enter an Administrator password. Use the password that you created when completing the New Virtual Machine wizard.

After installation is finished, VMware Tools is automatically installed.

Now that you have a virtual machine and with a guest operating system installed, you can refer to it as you read the rest of the topics in this chapter.

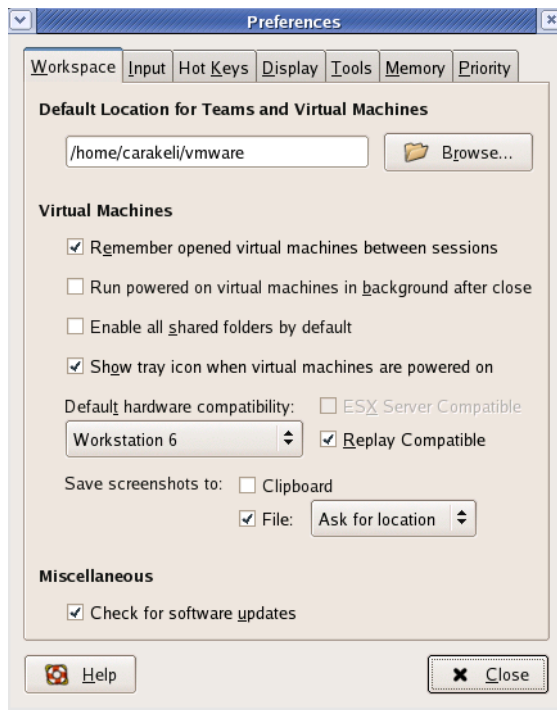
Introduction to Workstation Preferences

The Preferences dialog box appears when you choose **Edit > Preferences**. It lets you change a number of settings that apply to Workstation itself, no matter which virtual machine you are running.

The default settings for Workstation preferences are correct for most cases. Do not change settings unless you are an experienced user.

NOTE On a Linux host, you must be logged in as root to save global preference changes.

Figure 4-8 shows an example of the Workstation preferences editor.

Figure 4-8. Preference Editor's Workspace Tab (on a Linux Host)

Following is a list of the tabs in the Preferences dialog box, along with cross-references to the sections of this manual that pertain to each tab:

- **Workspace** tab – Lets you configure the following settings:
 - **Location** section – Lets you change the directory in which newly created virtual machines are stored. See [“Virtual Machine Location”](#) on page 88 and [“Files That Make Up a Virtual Machine”](#) on page 100.
 - **Virtual Machines** section – Several of these options have to do with exiting Workstation while leaving some virtual machines powered on. See [“Closing Virtual Machines and Exiting Workstation”](#) on page 81. For information about enabling shared folders, see [“Set Up Shared Folders”](#) on page 178.
 - **Software Updates** section – See [“Check for Product Updates”](#) on page 74.
- **Input** tab – Lets you adjust the way the virtual machine captures control of keyboard and mouse. For example, by default the virtual machine grabs keyboard and mouse input when you click in the virtual machine window.

- **Hot Keys** tab – Lets you specify the key combination that is used with hot-key sequences for all your virtual machines. Use hot-key sequences to enter and leave full screen mode, ungrab mouse and keyboard input, and so on.
- **Display** tab – Lets you adjust the manner in which the console and the host display accommodate a different guest operating system display resolution.

Also see [“Fitting the Workstation Console to the Virtual Machine Display”](#) on page 163 and [“Use Full Screen Mode”](#) on page 156.

- **Memory** tab – For details on adjusting memory settings in VMware Workstation, click the **Help** button on this tab. On Linux, you must be running Workstation as root in order to change the settings on the **Memory** tab of the preferences editor.
- **Priority** tab – For information about the snapshot settings on this tab, see [“Enable or Disable Background Snapshots”](#) on page 192. On Linux, you must be running Workstation as root in order to change this setting.

For information about the process priority settings available on Windows hosts, click the **Help** button on this tab.

- **Lockout** tab – (Windows hosts only) Lets you restrict who can create new virtual machines, edit virtual machine configurations, and change networking settings. For details, see [“Locking Out Interface Features for Windows Hosts Only”](#) on page 351.
- **Tools** tab – Lets you specify whether you want to automatically update VMware Tools on Windows and Linux guest systems when a new version becomes available. On Linux hosts, you must be running Workstation as root in order to change the settings on the **Tools** tab of the preferences editor.

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine by Workstation. See [Chapter 6, “Installing and Using VMware Tools,”](#) on page 103.

- **Devices** tab – (Windows hosts only) By default, the autorun feature mentioned on this tab is disabled. Therefore, you need to manually connect to the CD-ROM drive by using the **VM > Removable Devices** menu. See [“Use Removable Devices in a Virtual Machine”](#) on page 166.

In addition to the cross-references mentioned in this list, more information about the settings on each tab is available in the Workstation online help. Click **Help** in the Preferences dialog box.

The settings on the following tabs apply only to the user currently logged on to the host computer: **Workspace** tab, **Input** tab, **Hot Keys** tab, **Priority** tab, and **Tools** tab.

The settings on the following tabs apply no matter which virtual machine is running or which user is logged on to the host computer: **Display** tab, **Memory** tab, **Lockout** tab, and **Devices** tab.

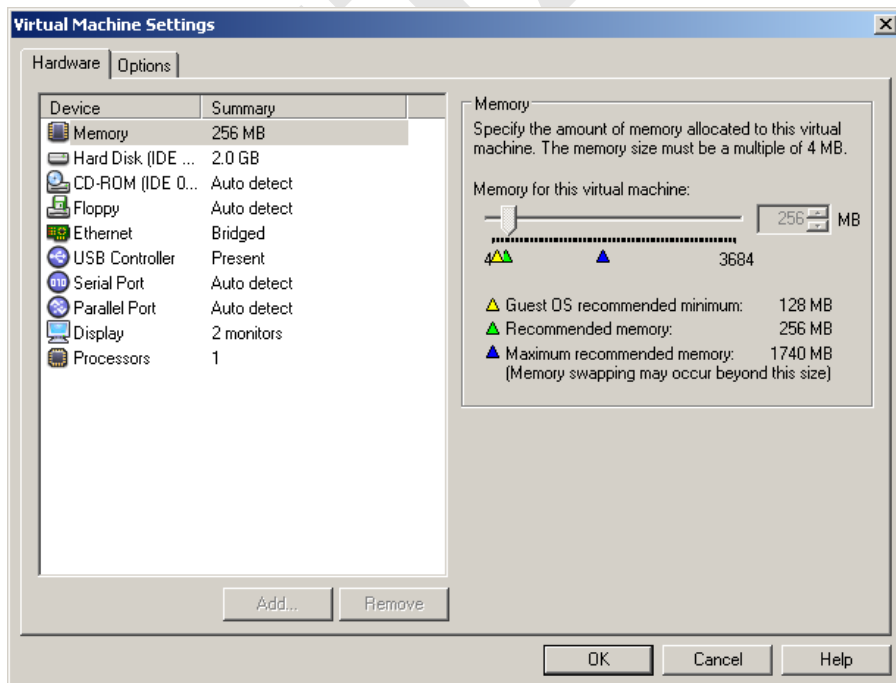
Introduction to Virtual Machine Settings

Workstation configures a new virtual machine based on the guest operating system you select in the New Virtual Machine wizard. After the virtual machine is created, you can use the virtual machine settings editor (**VM > Settings**) to change any configuration options set by the wizard. The virtual machine settings editor appears when you select a virtual machine and choose **VM > Settings**.

Hardware Tab

Use the **Hardware** tab to add, remove, and configure virtual devices for the selected virtual machine.

Figure 4-9. Virtual Machine Settings Hardware Tab



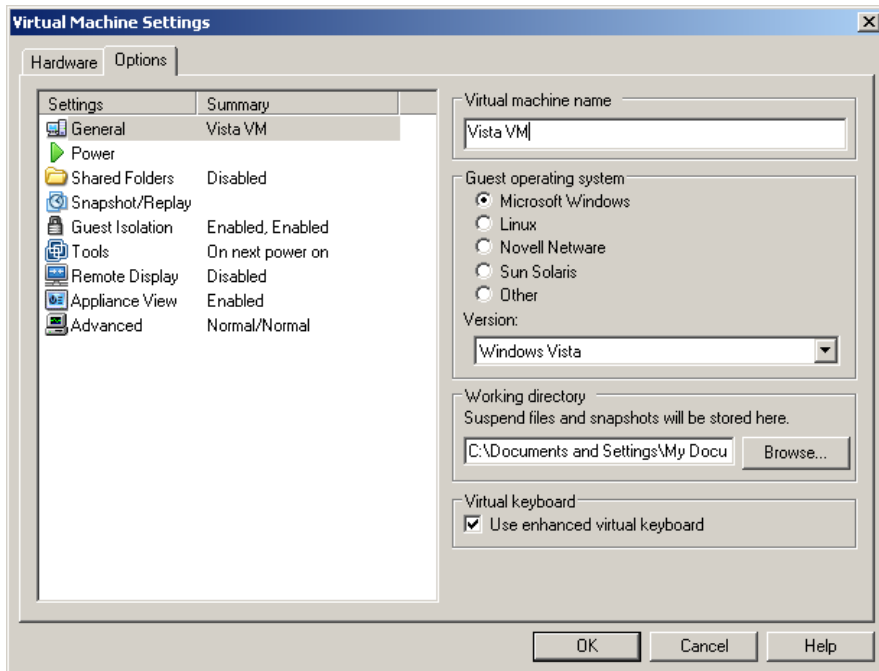
When you select an item in the hardware list, the options that correspond to the item are displayed on the right side of the dialog box. For example, in [Figure 4-9](#), memory options are displayed because the **Memory** item is selected.

Topics and chapters related to each of the virtual devices in the **Hardware** list are provided later in this manual. To display online help for an item you select in the **Hardware** list, click **Help** in the settings panel.

Options Tab

The **Options** tab lets you adjust characteristics of the selected virtual machine:

- Many options control interactions between the host and the guest operating system, such as how folders can be shared, how files are transferred, and what happens to a guest operating system when you exit Workstation.
- Some options let you override similar Preferences dialog box options, which are global preferences set for all virtual machines. For example, you can use the **Advanced** option to override the process priorities set on the **Priority** tab in the Preferences dialog box.
- Some options let you change settings you might initially make when running the New Virtual Machine wizard to create a virtual machine. For example, you can use the **General** options to change the name of the virtual machine.

Figure 4-10. Virtual Machine Settings Options Tab

The settings for the virtual machine **Options** tab are discussed later in this manual, in the task-specific topics and procedures where you would use them. To display online help for an item you select in the **Options** list, click **Help** in the settings panel.

Closing Virtual Machines and Exiting Workstation

When you close a virtual machine or team, and when you exit Workstation, if any virtual machines are still powered on, you are prompted to specify one of the following actions to take:

- Continue running the virtual machine in the background. If a virtual machine continues running after you exit Workstation, you can still interact with it through VNC or some other service.
- Suspend the virtual machine. The suspend operation saves the state of the virtual machine. See [“Using the Suspend and Resume Features”](#) on page 187.
- Power the virtual machine off. If you configured the power operation to do a “soft” power-off, a VMware Tools script runs in order to cleanly shut down the guest

operating system before powering off. See [“Configure Power Off and Reset Options for a Virtual Machine”](#) on page 152.

If you don't want to receive a prompt every time you exit Workstation or close a virtual machine or team, you can set a preference to specify that you want virtual machines to always run in the background when you exit.

Set a Virtual Machine to Run in the Background

When you close a virtual machine or team tab, or when you exit Workstation, if a virtual machine is still powered on, you can set it to continue running in the background. You can still interact with it through VNC or some other service.

By default, when virtual machines run in the background, a status icon is displayed in the notification area of the taskbar. Place your mouse pointer over the icon to display a tooltip that shows the number of virtual machines and teams that are running in the background. These are the virtual machines and teams that belong to the logged in user.

To set a virtual machine to run in the background

Do one of the following:

- Respond to the prompt when you close the virtual machine or exit Workstation, as follows: Click **Run in Background**.
- Set a Workstation preference:
 - a From the VMware Workstation menu bar, choose **Edit > Preferences**.
 - b On the **Workspace** tab, select **Run powered on virtual machines in background after close** and click **OK**.

When you close a tab or exit Workstation, you no longer receive a prompt.

Keyboard Shortcuts

If you prefer to work from the keyboard, use the keyboard shortcuts shown in [Table 4-1](#). If you changed the Preferences setting for the hot-key combination, substitute your new setting for Ctrl+Alt as needed in the shortcuts listed in [Table 4-1](#).

Table 4-1. Keyboard Shortcuts

Shortcut	Action
Ctrl+B	Power on.
Ctrl+E	Power off.
Ctrl+R	Reset the power.

Table 4-1. Keyboard Shortcuts (Continued)

Shortcut	Action
Ctrl+Z	Suspend.
Ctrl+N	Create a new virtual machine.
Ctrl+O	Open a virtual machine.
Ctrl+F4	Close the summary/console view for the selected virtual machine. A confirmation dialog appears only if the virtual machine is powered on.
Ctrl+D	Edit the virtual machine's configuration.
F9	Toggle between displaying and hiding the sidebar.
Ctrl+G	Grab input from keyboard and mouse.
Ctrl+P	Edit preferences.
Ctrl+Alt+Enter	Toggle between full screen mode and windowed mode.
Ctrl+Alt	Release the mouse cursor. If the virtual machine is in the type of full screen mode called exclusive mode, pressing Ctrl+Alt brings the virtual machine out of exclusive mode and into full screen mode.
Ctrl+Alt+Tab	Switch among open virtual machines while mouse and keyboard input are grabbed.
Ctrl+Tab	Switch among open virtual machines while mouse and keyboard input are not grabbed. VMware Workstation must be the active application.
Ctrl+Shift+Tab	Switch among open virtual machines while mouse and keyboard input are not grabbed. VMware Workstation must be the active application.
Ctrl+Shift+right arrow	In full screen mode, switch to the next powered-on virtual machine.
Ctrl+Shift+left arrow	In full screen mode, switch to the previous powered-on virtual machine.

BETA

Creating a Virtual Machine

This chapter describes how to create a virtual machine by using the New Virtual Machine wizard. It provides general information about installing guest operating systems. This chapter includes the following topics:

- [“Methods of Creating Virtual Machines”](#) on page 85
- [“Configuration Options for the New Virtual Machine Wizard”](#) on page 86
- [“Using the New Virtual Machine Wizard”](#) on page 92
- [“Install a Guest Operating System Manually”](#) on page 96
- [“Upgrade a Guest Operating System”](#) on page 99
- [“Files That Make Up a Virtual Machine”](#) on page 100

Methods of Creating Virtual Machines

Workstation gives you several options for creating virtual machines:

- Create a virtual machine from scratch.

If you do not have any virtual machines or system images, you must use this method. Use the New Virtual Machine wizard to create a virtual machine. Next, you must install an operating system. The process is the same as installing it on a physical computer.

The rest of this chapter describes this method of creating a virtual machine.

- Clone a virtual machine from an existing VMware virtual machine or virtual machine template.

Clones are useful when you must deploy many identical virtual machines to a group. Cloning is preferable to copying a virtual machine because a clone’s MAC

address and UUID are different from the original virtual machine, to avoid network conflicts. Use the Clone Virtual Machine wizard to create a clone.

See [“Cloning a Virtual Machine”](#) on page 201.

- Convert a physical machine, virtual machine, or system image that was created by using another VMware product or a third-party product.

This process creates a clone of the original virtual machine or system image. Use the Converter Import wizard to convert a physical or virtual machine or a system image.

See [Chapter 7, “Creating a Virtual Machine from a System Image or Another Virtual Machine,”](#) on page 137.

Configuration Options for the New Virtual Machine Wizard

As you complete the New Virtual Machine wizard, you are prompted to make decisions about many aspects of the virtual machine. The topics in this section provide information about the issues involved so that you can determine which choices you want to make before running the wizard.

Easy Install Feature for Windows Guest Operating Systems

The easy install features enables you to perform an unattended installation of the guest operating system after you complete the New Virtual Machine wizard. It also installs VMware Tools in the guest operating system. For more information about VMware Tools, see [“Components of VMware Tools”](#) on page 103. You can select this option regardless of whether you choose a typical or a custom configuration in the New Virtual Machine wizard.

If you plan to use a CD, DVD, or ISO image that contains a product key number and is already set up to perform an unattended installation, the only benefit you gain by using the easy install feature is the automatic installation of VMware Tools.

For this release, the easy install feature is available for the following operating systems: Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. The installation media that you can use include operating system installation CDs, DVDs, and ISO images.

Typical Versus Custom Configurations

The New Virtual Machine wizard prompts you to choose between doing a typical configuration and a custom configuration. If you select **Typical**, the wizard prompts you to specify or accept defaults for the following choices:

- Medium for installing the guest operating system (CD, image file, or neither)
- Guest operating system
- Virtual machine name and the location of the virtual machine files
- Size of the virtual disk
- Hardware customization, for advanced users

You are not prompted to specify the virtual machine version. The virtual machine version (Workstation 4, 5, 6, or 6.5) is assumed to be the one specified in the preferences editor. From the Workstation menu bar, choose **Edit > Preferences**, and see the setting for **Default hardware compatibility**.

On the last page of the wizard, you can click **Customize Hardware** to change the defaults for memory allocation, number of virtual CPUs, network connection type, and so on.

Many circumstances require you to select a custom installation. Select **Custom** if you want to do any of the following:

- Make a different version of virtual machine than what is specified in the preferences editor.
- Specify the I/O adapter type for SCSI adapters: BusLogic or LSI Logic.
- Specify whether you want to create an IDE or a SCSI virtual disk, regardless of the default that is usually used for the guest operating system.

To determine the type of virtual disk that is displayed by default for a particular operating system, select the **Custom** option and click **Next** through the wizard pages, select the guest operating system, and continue through the wizard until you get to the Select a Disk Type page. The default is already selected.

- Use a physical disk rather than a virtual disk (for expert users).
- Use an existing virtual disk rather than create a new virtual disk.
- Place the virtual disk file in a location other than the virtual machine directory.
- Allocate all virtual disk space rather than allowing the disk space to gradually grow to the maximum.
- Split the virtual disk into 2 GB files.

Guest Operating System Selection

The New Virtual Machine wizard prompts you to specify which type of operating system you plan to install in the guest. You can choose Windows 2000 Professional, Red Hat Linux 4, Ubuntu 64-bit, and many others. Workstation uses this information to do the following:

- Select appropriate default values, such as the amount of memory to allocate.
- Name files associated with the virtual machine.
- Adjust settings for optimal performance.
- Work around special behaviors and bugs within a guest operating system.

If the operating system you plan to use is not listed, select **Other** for both guest operating system and version.

For some Windows operating systems, if you supply the installation media and the wizard detects it, the operating system and VMware Tools are installed automatically after the virtual machine is created. See [“Easy Install Feature for Windows Guest Operating Systems”](#) on page 86.

NOTE Workstation supports 64-bit guest operating systems only in Workstation versions 5.5 and later, and only on host machines with supported processors. For the list of processors Workstation supports for 64-bit guest operating systems, see [“PC Hardware”](#) on page 26.

Virtual Machine Location

The following examples show the default locations suggested for virtual machines.

- On Windows 2000, Windows XP, and Windows Server 2003, the default folder for a Windows XP Professional virtual machine is:

```
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\Windows XP Professional
```

- On Windows Vista, the default folder is:

```
C:\Users\<username>\Documents\Virtual Machines\Windows XP Professional
```

- On Linux hosts, the default location for a Windows XP Professional virtual machine is:

```
<homedir>/vmware/Windows XP Professional
```

where <homedir> is the home directory of the user who is currently logged on.

Virtual machine performance might be slower if your virtual hard disk is on a network drive. For best performance, be sure the virtual machine's folder is on a local drive. However, if other users need to access this virtual machine, consider placing the virtual machine files in a location that is accessible to them. See [“Sharing Virtual Machines with Other Users”](#) on page 209.

For information about the files stored in the virtual machine folder, see [“Files That Make Up a Virtual Machine”](#) on page 100.

Number of Processors

This option is available for custom configurations only. Setting the virtual machine to have two processors is supported only for host machines with at least two logical processors. (If you are creating a Workstation 4 virtual machine, you do not see this panel.)

The following are all considered to have two logical processors:

- A single-processor host with hyperthreading enabled
- A single-processor host with a dual-core CPU
- A multiprocessor host with two CPUs, regardless of whether they are dual-core or have hyperthreading enabled

Network Connection Type

This option is available for custom configurations or if you click **Customize Hardware** on the last page of the New Virtual Machine wizard. You have several options for connecting the virtual machine to the network:

- **Bridged networking** – If your host computer is on a network and you have a separate IP address for your virtual machine (or can get one automatically from a DHCP server), select **Use bridged networking**. Other computers on the network can then communicate directly with the virtual machine.
- **NAT** – If you do not have a separate IP address for your virtual machine but you want to be able to connect to the Internet, select **Use network address translation (NAT)**. The virtual machine and the host share a single network identity that is not visible outside the network.
- **Host-only** – Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual Ethernet adapter that is visible to the host operating system. With host-only networking, the virtual machine can communicate only with the host and other virtual machines in the

host-only network. This approach can be useful if you need to set up an isolated virtual network.

- **No connection** – You can always set up a connection after you finish creating the virtual machine.

See [“Common Networking Configurations”](#) on page 260.

SCSI Adapter Types

This option is available for custom configurations only. An IDE and a SCSI adapter are installed in the virtual machine. The IDE adapter is always ATAPI. For the SCSI adapter, you can choose BusLogic or LSI Logic. The default for your guest operating system is already selected. All guests except for Windows Vista, Windows Server 2003, Red Hat Enterprise Linux 3, and NetWare default to the BusLogic adapter. For Windows Vista guests, your only choice is LSI Logic.

NOTE The LSI Logic adapter has improved performance and works better with generic SCSI devices. The LSI Logic adapter is also supported by ESX Server 2.0 and higher.

Your choice of SCSI adapter does not affect your decision to make your virtual disk an IDE or SCSI disk. However, some guest operating systems, such as 32-bit Windows XP, do not include a driver for the Buslogic or LSI Logic adapter. You must download the driver from the LSI Logic Web site.

NOTE Drivers for a Mylex (BusLogic) compatible host bus adapter are not obvious on the LSI Logic Web site. Search the support area for the numeric string in the model number. For example, search for “958” for BT/KT-958 drivers.

See the *VMware Guest Operating System Installation Guide* for details about the driver and the guest operating system you plan to install in this virtual machine.

Normal and Independent Disk Modes

The option to select normal or independent mode is available on Linux hosts for custom configurations only. Normal mode means you want to include disks in any snapshots you take. If you do not want data on the disk to be recorded when you take a snapshot of the virtual machine, you can configure the disk to be independent.

If you configure the disk to be independent, you can further specify whether changes you make to the disk are to persist or be discarded when you power off the virtual machine or restore it to a snapshot.

Although for Windows hosts, this configuration setting is not available in the New Virtual Machine wizard, you can exclude virtual disks from snapshots by using the virtual machine settings editor. See [“Exclude a Virtual Disk from Snapshots”](#) on page 192.

Virtual Disks and Physical Disks

This option is available for custom configurations only. If you use a typical configuration, a new virtual disk is created and used for the virtual machine. Virtual disks are the best choice for most virtual machines. They are easy to set up and can be moved to new locations on the same host computer or to different host computers.

Even for custom configurations, you usually choose the option **Create a New Virtual Disk**. In some cases you might want to choose **Use an Existing Virtual Disk**, to use a virtual disk you created previously. The wizard displays a page for you to enter the path or browse to the existing virtual disk (.vmdk) file.

It is possible to use a physical hard disk (a “raw” disk) or IDE disk partition in a virtual machine. Do not use a physical disk configuration unless you are an expert user. See [“Using Physical Disks in a Virtual Machine”](#) on page 221.

Disk Capacity

The wizard prompts you to set a size between 0.1GB and 950GB for a virtual disk. For custom configurations, you can also choose whether to allocate all the disk space now or allow the virtual machine to grow as you use it. VMware recommends that you allow the disk to grow.

The option **Allocate all disk space now** gives somewhat better performance for your virtual machine, but it is a time-consuming operation that cannot be canceled. Also it requires as much physical disk space as you specify for the virtual disk. If you allocate all the disk space now, you cannot use the shrink disk feature later.

For custom configurations, you are also given the option **Split disk into 2GB files**. Select this option if your virtual disk is stored on a file system that does not support files larger than 2GB.

Pocket ACE Disk Size Calculator on Windows Only

The Pocket ACE feature allows you to store ACE instances on portable devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, and portable hard drives. ACE users attach these portable devices to x86 host computers and run their ACE instances with VMware Player.

On the Specify Disk Capacity page of the New Virtual Machine wizard, you can use the **Calculate optimal size for Pocket ACE** button to determine what number to use in the **Disk size** text box. Disk size refers only to the size of the virtual hard disk. If you plan to create Pocket ACEs, you must also consider the amount of disk space required for memory, installers, and other files related to virtual machine overhead.

To determine what number to enter in the **Space available** text box of the calculator, plug the USB device in to your host computer and use the My Computer item to display its properties.

Using the New Virtual Machine Wizard

The New Virtual Machine wizard guides you through the key steps for setting up a new virtual machine, helping you set various options and parameters.

Many of the settings you specify in the New Virtual Machine can be changed later, if necessary. You can use the virtual machine settings editor if you need to make changes after the initial creation. (From the menu bar, choose **VM > Settings**.)

The New Virtual Machine wizard prompts you to choose between doing a typical or custom setup.

Before you begin, determine what type of media to use for installing the operating system in the virtual machine and do one of the following:

- If you plan to use an installation CD or DVD for installing the guest operating system, insert the CD or DVD in the host's CD-ROM drive.
- If you plan to use an ISO image file, make sure the file is accessible to the host.

Create a Virtual Machine by Using the Typical Setup

If you are not sure whether to use this procedure, see [“Typical Versus Custom Configurations”](#) on page 87.

To create a virtual machine by using the typical setup

- 1 From the Workstation menu bar, choose **File > New > Virtual Machine**, to start the New Virtual Machine wizard.
- 2 On the Welcome page, select **Typical** and click **Next**.
- 3 On the Guest Operating System Installation page, specify the location of the operating system installation media and click **Next**.

If you select **Installer disc** or **Installer disc image file** and if the wizard can detect the operating system, you might not see a wizard page for selecting the operating system.

- 4 If the Select a Guest Operating System page appears, select the operating system (including the version) to install and click **Next**.
- 5 If the Easy Install Information page appears, specify the following and click **Next**:
 - (Optional) **The product key** – If you specify a product key, you are not prompted for it later, during installation of the operating system. Enter a product key even if the installation media already contains a product key.
 - **A name for registering the operating system** – For Windows guests, do not use the name Administrator or Guest. If you use one of these names, you will receive an error message during installation of the operating system and be prompted to enter a different name.
 - (Optional) **Password** – On Windows operating systems other than Windows 2000, the password you enter here is used for an account with Administrator permissions. On Windows 2000, the password you enter here is used for the Administrator account.

This page appears for some Windows operating systems.

- 6 On the Name the Virtual Machine page, type a name, select a folder for the virtual machine, and click **Next**.

The name you provide here is used if you add this virtual machine to the VMware Workstation **Favorites** list. This name is also used as the name of the folder where all the files associated with this virtual machine are stored.

- 7 On the Specify Disk Capacity page, enter the size of the virtual disk and click **Next**.

See [“Disk Capacity”](#) on page 91 and [“Pocket ACE Disk Size Calculator on Windows Only”](#) on page 91.

- 8 (Optional) On the Ready to Create Virtual Machine page, if you want to change or add virtual hardware devices, click **Customize Hardware**.

The virtual hardware settings editor appears. For information about the settings panels in this editor, click **Help** in the dialog box.

- 9 Click **Finish**.

If you entered easy install information, the unattended installation of the operating system and VMware Tools begins.

After the virtual machine is created, if you did use the easy install feature, continue on to [“Install a Guest Operating System Manually”](#) on page 96.

Create a Virtual Machine by Using the Custom Setup

If you are not sure whether to use this procedure, see [“Typical Versus Custom Configurations”](#) on page 87.

Before you begin, determine what type of media to use for installing the operating system in the virtual machine and do one of the following:

- If you plan to use an installation CD or DVD for installing the guest operating system, insert the CD or DVD in the host's CD-ROM drive.
- If you plan to use an ISO image file, make sure the file is accessible to the host.

To create a virtual machine by using the custom setup

- 1 From the Workstation menu bar, choose **File > New > Virtual Machine**, to start the New Virtual Machine wizard.
- 2 On the Welcome page, select **Custom** and click **Next**.
- 3 On the Choose the Virtual Machine Hardware Compatibility page, specify whether you want to create a Workstation 4, 5, 6, or 6.5 virtual machine, select the appropriate compatibility check boxes, and click **Next**.

When you make a selection from the **Hardware Compatibility** list, you see a list of other VMware products and versions that are compatible with your selection. You also see a list of features that are not available for that version.

If one of the feature compatibility check boxes is available for the version you select, you can select the check box to see a list of the additional limitations.

- 4 On the Guest Operating System Installation page, specify the location of the operating system installation media and click **Next**.

If you select **Installer disc** or **Installer disc image file** and if the wizard can detect the operating system, you might not see a wizard pages for selecting the operating system.

- 5 If the Select a Guest Operating System page appears, select the operating system (including the version) to install and click **Next**.
- 6 If the Easy Install Information page appears, specify the following and click **Next**:
 - (Optional) **The product key** – If you specify a product key, you are not prompted for it later, during installation of the operating system. Enter a product key even if the installation media already contains a product key.

- **A name for registering the operating system** – For Windows guests, do not use the name Administrator or Guest. If you use one of these names, you will receive an error message during installation of the operating system and be prompted to enter a different name.
- (Optional) **Password** – On Windows operating systems other than Windows 2000, the password you enter here is used for an account with Administrator permissions. On Windows 2000, the password you enter here is used for the Administrator account.

This page appears for some Windows operating systems.

- 7 On the Name the Virtual Machine page, type a name, select a folder for the virtual machine, and click **Next**.

The name you provide here is used if you add this virtual machine to the VMware Workstation **Favorites** list. This name is also used as the name of the folder where all the files associated with this virtual machine are stored.

- 8 If the Processor Configuration page appears, select the number of processors for the virtual machine and click **Next**.

This page does not appear if you are creating a Workstation 4 virtual machine or if you selected the **Compatible with Replay** check box.

- 9 On the Memory for the Virtual Machine page, either adjust the memory settings or accept the default setting and click **Next**.

If you plan to use the virtual machine to run many applications or applications that need large amounts of memory, you might want to use a higher memory setting.

You cannot allocate more than 2GB of memory to a virtual machine if the virtual machine's files are stored on file systems such as Windows 9.x and ME with FAT16 that do not support files greater than 2GB.

- 10 On the Network Type page, configure the networking capabilities of the virtual machine and click **Next**.

See [“Network Connection Type”](#) on page 89.

- 11 On the Select I/O Adapter Types page, select the type of SCSI adapter you want to use with the virtual machine and click **Next**.

See [“SCSI Adapter Types”](#) on page 90.

- 12 On the Select a Disk page, select whether to create an IDE or SCSI disk and click **Next**.

For more information, see [“Virtual Disks and Physical Disks”](#) on page 91.

- 13 On the Select a Disk Type page, select whether to create an IDE or SCSI disk and click **Next**.

The default is based on the guest operating system you selected. All Linux distributions you can select in the wizard use SCSI virtual disks by default, as do several newer Windows operating systems and 64-bit operating systems.

See [“SCSI Adapter Types”](#) on page 90.

- 14 On Linux hosts only, on the Select a Disk Type page, if you want to exclude disks from snapshots, in the **Mode** section, select **Independent** for the mode and choose one of the following options:

- **Persistent** – Changes are immediately and permanently written to the disk.
- **Nonpersistent** – Changes to the disk are discarded when you power off or revert to a snapshot.

See [“Exclude a Virtual Disk from Snapshots”](#) on page 192.

- 15 On the Specify Disk Capacity page, enter the size of the virtual disk, specify the way you want the disk space allocated, and click **Next**.

See [“Disk Capacity”](#) on page 91 and [“Pocket ACE Disk Size Calculator on Windows Only”](#) on page 91.

- 16 On the Specify Disk File page, enter the location of the virtual disk's files and click **Next**.

- 17 (Optional) On the Ready to Create Virtual Machine page, if you want to change or add virtual hardware devices, click **Customize Hardware**.

The virtual hardware settings editor appears. For more information about the settings panels in this editor, click **Help** in the dialog box.

- 18 Click **Finish**.

If you entered easy install information, the unattended installation of the operating system and VMware Tools begins.

After the virtual machine is created, if you did use the easy install feature, continue on to [“Install a Guest Operating System Manually”](#) on page 96.

Install a Guest Operating System Manually

Perform the procedure described in this topic if you did not select the easy install feature when using the New Virtual Machine wizard.

A new virtual machine is like a physical computer with a blank hard disk. Before you can use it, you need to partition and format the virtual disk and install an operating system. The operating system's installation program might handle the partitioning and formatting steps for you.

Installing a guest operating system inside your VMware Workstation virtual machine is essentially the same as installing it on a physical computer.

NOTE Workstation supports 64-bit guest operating systems only in Workstation versions 5.5 and later, and only on host machines with supported processors. For the list of processors Workstation supports for 64-bit guest operating systems, see [“PC Hardware”](#) on page 26.

For information about installing a Linux operating system that has a VMware VMI (Virtual Machine Interface) enabled kernel in the guest operating system, see [“Use a Paravirtualized Kernel in Linux Guests to Enhance Performance”](#) on page 98.

To install a guest operating system manually

- 1 Start VMware Workstation.
- 2 Do one of the following so that the virtual machine can access the installation media for the guest operating system:
 - For a CD or DVD, if necessary, configure the virtual machine to use the host's CD-ROM/DVD drive, and insert the operating system media in the drive.

In some host configurations, the virtual machine cannot boot from the installation CD-ROM. You can work around that problem by creating an ISO image file from the installation CD-ROM. Use the virtual machine settings editor (choose **VM>Settings**) to connect the virtual machine's CD drive to the ISO image file, and power on the virtual machine.

- For an .ISO image, connect the CD-ROM drive to an .ISO image file of an installation disk.

To use a PXE server to install the guest operating system over a network connection, you do not need the operating system installation media. When you power on the virtual machine (in the next step), the virtual machine detects the PXE server.

- 3 If the operating system spans several CDs, follow these steps when you are prompted to insert the second CD:
 - a Disconnect from the current image by choosing **VM>Removable Devices>CD-ROM>Disconnect**.
 - b Edit the CD settings by choosing **VM>Removable Devices>CD-ROM>Edit**.
 - c For **Use ISO image file**, click **Browse**, and select the ISO image for the second CD.
 - d In the **Device Status** area, select the **Connected** check box and click **OK**.
 - e In the guest operating system, click **OK** or respond to the prompt so that installation can continue.
 - f Repeat this process for additional CDs.
- 4 Click the **Power On** button.
- 5 Follow the instructions provided by the operating system vendor.

Also see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the **Help** menu.

After the guest operating system is installed, you can use the standard tools within the operating system to configure its settings. VMware recommends that you install VMware Tools before you activate the license for the operating system. See “[Installing VMware Tools](#)” on page 105.

Use a Paravirtualized Kernel in Linux Guests to Enhance Performance

Since 2005, VMware has been collaborating with the Linux community to develop a common paravirtualization interface. In 2006, VMware released its VMI specification as an open specification. For more information about paravirtualization in general, see the following VMware Web site at:

<http://www.vmware.com/interfaces/paravirtualization.html>

If you have a VMware VMI (Virtual Machine Interface) enabled kernel in the guest operating system, you will see improved performance if you enable paravirtual support in the virtual machine.

To get and enable a paravirtualized kernel

- 1 To get a VMI-enabled kernel, download the CD image of Ubuntu 7.04 (Feisty) or later from:
<http://www.ubuntu.com/getubuntu/download>
Use the standard image for 32-bit Intel x86 computers. VMI is currently 32-bit only.
- 2 Use Workstation's New Virtual Machine wizard to create a Workstation 6 or higher virtual machine with the guest operating system type **Ubuntu**.
See "Using the New Virtual Machine Wizard" on page 92. Make sure the hardware version is Workstation 6.
- 3 After you finish creating the virtual machine, enable paravirtual kernel support, as follows:
 - a From the Workstation menu bar, choose **VM>Settings**.
The virtual machine settings editor opens.
 - b On the **Options** tab, click **Advanced**, and in the **Settings** section, select the **Enable VMware paravirtual kernel support** check box.
Do not close the virtual machine settings editor.
- 4 Set the virtual machine to use the ISO image you downloaded in [Step 1](#):
 - a On the **Hardware** tab, select **CD-ROM**, and in the **Connection** section, select **Use ISO image**.
 - b Browse to and select the ISO image you downloaded in [Step 1](#).
 - c Click **OK** to save your settings and close the virtual machine settings editor.
- 5 Power on the virtual machine and install the Linux operating system from the ISO file.

Upgrade a Guest Operating System

When you use the New Virtual Machine wizard to create a virtual machine, one of the settings you specify is the guest operating system type and version. Workstation chooses configuration defaults based on the guest type and version you choose.

If you upgrade a guest operating system to a newer version, also update the guest operating system version for the virtual machine.

To upgrade a guest operating system

- 1 Start Workstation and select the virtual machine.
Make sure the virtual machine is powered off.
- 2 From the Workstation menu bar, choose **VM>Settings**.
- 3 In the virtual machine settings editor, click **Options**.
- 4 On the **General** settings panel, in the **Version** field, select the version to which you plan to upgrade and click **OK**.

The setting you specify here is written to the virtual machine's configuration file. This setting does not actually change the guest operating system itself.
- 5 Power on the virtual machine.
- 6 To upgrade the guest operating system, follow the upgrade instructions provided by the operating system vendor.

Files That Make Up a Virtual Machine

You might never need to know the filenames or locations for your virtual machine files. Virtual machine file management is performed by Workstation.

A virtual machine typically is stored on the host computer in a set of files, usually in a directory created by Workstation for that specific virtual machine. See [“Virtual Machine Location”](#) on page 88.

The key files are listed in [Table 5-1](#) by extension. In these examples, <vmname> is the name of your virtual machine.

Table 5-1. Virtual Machine Files

Extension	File Name	Description
.log	<vmname>.log or vmware.log	The log file of key Workstation activity. This file is useful in troubleshooting. This file is stored in the directory that holds the configuration (.vmx) file of the virtual machine.
.nvram	<vmname>.nvram or nvram	The NVRAM file, which stores the state of the virtual machine's BIOS.

Table 5-1. Virtual Machine Files (Continued)

Extension	File Name	Description
.vmdk	<vmname>.vmdk	<p>VMDK files, which store the contents of the virtual machine's hard disk drive.</p> <p>A virtual disk is made up of one or more virtual disk (.vmdk) files. The virtual machine settings editor shows the name of the first file in the set. This file contains pointers to the other files in the set.</p> <p>(If you specify that all space should be allocated when you create the disk, these files start at the maximum size and do not grow.) Almost all of a .vmdk file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead.</p> <p>If the virtual machine is connected directly to a physical disk, the .vmdk file stores information about the partitions the virtual machine is allowed to access.</p> <p>Earlier VMware products used the extension .disk for virtual disk files.</p>
.vmdk Continued	<vmname>-s<###>.vmdk	<p>If you specified that the files can grow, the filenames include an s in the file number (for example, Windows XP Professional-s001.vmdk.)</p> <p>If you specified that the virtual disk is split into 2GB chunks, the number of .vmdk files depends on the size of the virtual disk. As data is added to a virtual disk, the .vmdk files grow, to a maximum of 2GB each.</p>
	<vmname>-f<###>.vmdk	<p>If the disk space was allocated when the disk was created, the names include an f instead of an s (for example, Windows XP Professional-f001.vmdk).</p>
	<vmname>-<disk>-<###>.vmdk	<p>If the virtual machine has one or more snapshots, some files are redo-log files. They store changes made to a virtual disk while the virtual machine is running. The ### indicates a unique suffix added by VMware Workstation to avoid duplicate file names.</p>
.vmem	<uuid>.vmem	<p>The virtual machine's paging file, which backs up the guest main memory on the host file system. This file exists only when the virtual machine is running or if the virtual machine fails.</p>
	<snapshot_name_number>.vmem	<p>Each snapshot of a virtual machine that is powered on has an associated .vmem file, which contains the guest's main memory, saved as part of the snapshot.</p>

Table 5-1. Virtual Machine Files (Continued)

Extension	File Name	Description
.vmsd	<vmname>.vmsd	A centralized file for storing information and metadata about snapshots.
.vmsn	<vmname>-Snapshot.vmsn	The snapshot state file, which stores the running state of a virtual machine at the time you take that snapshot.
	<vmname>-Snapshot<###>.vmsn	The file that stores the state of a snapshot.
.vmss	<vmname>.vmss	The suspended state file, which stores the state of a suspended virtual machine. Some earlier VMware products used the extension .std for suspended state files.
.vmtm	<vmname>.vmtm	The configuration file containing team data.
.vmx	<vmname>.vmx	The primary configuration file, which stores settings chosen in the New Virtual Machine wizard or virtual machine settings editor. If you created the virtual machine under an earlier version of VMware Workstation on a Linux host, this file might have a .cfg extension.
.vmxf	<vmname>.vmxf	A supplemental configuration file for virtual machines that are in a team. Note that the .vmxf file remains if a virtual machine is removed from the team.

Other files might be present in the directory. Some are present only while a virtual machine is running. See [“Lock Files”](#) on page 214.

Installing and Using VMware Tools

6

This chapter discusses how to install, update, and run VMware Tools. This chapter includes the following topics:

- [“Components of VMware Tools”](#) on page 103
- [“Installing VMware Tools”](#) on page 105
- [“VMware Tools Update Process”](#) on page 117
- [“Uninstall VMware Tools”](#) on page 120
- [“Repair or Change Installed Modules”](#) on page 120
- [“Open the VMware Tools Control Panel”](#) on page 121
- [“Configure VMware Tools in a NetWare Guest”](#) on page 126
- [“Customizations to VMware Tools”](#) on page 127
- [“Use the VMware Tools Command-Line Interface”](#) on page 133

Components of VMware Tools

VMware Tools is a suite of utilities that enhances the performance of the virtual machine’s guest operating system and improves management of the virtual machine. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience.

VMware Tools includes the following components:

- VMware Tools service
- VMware device drivers

- VMware user process
- VMware Tools control panel

VMware Tools Service

The program file is called `VMwareService.exe` on Windows guest operating systems and `vmware-guestd` on Linux, FreeBSD, and Solaris guests.

This service performs various duties within the guest operating system:

- Passes messages from the host operating system to the guest operating system.
- Executes commands in the operating system to cleanly shut down or restart a Linux, FreeBSD, or Solaris system when you select power operations in Workstation.
- Sends a heartbeat to a VMware Server, if you use the virtual machine with VMware Server.
- On Windows guests, grabs and releases the mouse cursor.
- On Windows guests, fits the guest's screen resolution to the host's screen resolution and the reverse.
- Synchronizes the time in the guest operating system with the time in the host operating system.
- Runs scripts that help automate guest operating system operations. The scripts run when the virtual machine's power state changes.

The service starts when the guest operating system boots.

The VMware Tools service is not installed on NetWare operating systems. Instead, the `vmwtool` program is installed. It synchronizes time and allows you to turn the CPU idler on or off.

VMware Device Drivers

These drivers include:

- SVGA display driver that provides high display resolution and significantly faster overall graphics performance.
- The `vmxnet` networking driver for some guest operating systems.
- BusLogic SCSI driver for some guest operating systems.
- VMware mouse driver.

- A kernel module for handling shared folders, called `hgfs.sys` on Windows and `vmhgfs` on Linux and Solaris.
- The Virtual Machine Communication Interface (VMCI) driver for creating client-server applications that are optimized for fast and efficient communication between virtual machines.

VMware User Process

The program file is called `VMwareUser.exe` on Windows guests and `vmware-user` on Linux and Solaris guests.

This service performs the following tasks within the guest operating system:

- Enables you to copy and paste text between the guest and host operating systems, and copy and paste files between the host operating systems and Windows, Linux, and Solaris guest operating systems.
- Enables you to drag and drop files between the host operating systems and Windows, Linux, and Solaris guest operating systems.
- On Linux and Solaris guests, grabs and releases the mouse cursor when the SVGA driver is not installed.
- On Linux and Solaris guests, fits the guest's screen resolution to the host's.

The VMware Tools user process is not installed on NetWare operating systems. Instead, the `vmwtool` program is installed. It controls the grabbing and releasing of the mouse cursor. It also allows you copy and paste text. You cannot drag and drop or copy and paste files between hosts and NetWare guest operating systems.

VMware Tools Control Panel

The VMware Tools control panel lets you modify settings, shrink virtual disks, and connect and disconnect virtual devices. See [“Open the VMware Tools Control Panel”](#) on page 121.

Installing VMware Tools

The installers for VMware Tools for Windows, Linux, FreeBSD, Solaris, and NetWare guest operating systems are installed with VMware Workstation as ISO image files. When you choose **VM > Install VMware Tools** from the VMware Workstation menu bar, Workstation temporarily connects the virtual machine's first virtual CD-ROM drive to the correct ISO image file for the guest operating system.

You can use this menu command to either install or update VMware Tools. The installation procedure varies depending on the operating system:

- [“Manually Install VMware Tools in a Windows Guest Operating System”](#) on page 106
- [“Install VMware Tools on a Linux Guest Within X by Using the RPM Installer”](#) on page 110
- [“Install VMware Tools from the Command Line with the Tar or RPM Installer”](#) on page 111
- [“Install VMware Tools in a Solaris Guest”](#) on page 113
- [“Install VMware Tools in a FreeBSD Guest”](#) on page 114
- [“Install VMware Tools in a NetWare Virtual Machine”](#) on page 116

Manually Install VMware Tools in a Windows Guest Operating System

VMware Tools is supported on all Windows guest operating systems.

Before you use the menu command to install VMware Tools, perform the following tasks, as necessary:

- If you are running Workstation on a Windows host and your virtual machine has only one CD-ROM drive, make sure the CD-ROM drive is configured as an IDE or SCSI CD-ROM drive. It cannot be configured as a generic SCSI device. If necessary, add an IDE or SCSI CD-ROM drive to the virtual machine. See [“Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine”](#) on page 227.
- Make sure the virtual CD-ROM drive is configured to auto-detect a physical drive. This task is necessary if you connected the virtual machine's CD drive to an ISO image file when you installed the operating system. Change the connection from the ISO image to auto-detect a physical drive. (With the virtual machine powered off, choose **VM > Settings > CD-ROM > Use Physical Drive, Auto-detect.**)
- When you install VMware Tools, make sure the virtual machine is powered on.
- If the guest operating system is a Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista operating system, log in as an administrator. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows Me guest operating system.

To install VMware Tools

- 1 On the host, from the Workstation menu bar, choose **VM > Install VMware Tools**.

Depending on whether autorun is enabled, one of the following occurs inside the guest operating system:

- If autorun is enabled in the guest operating system, a dialog box appears after a few seconds. It asks whether you want to install VMware Tools.
- If autorun is not enabled, the dialog box does not appear automatically. Click **Start > Run** and enter **D:\setup\setup.exe** where **D:** is your first virtual CD-ROM drive.

- 2 Click **Yes** to launch the InstallShield wizard.

- 3 Follow the on-screen instructions.

On some Windows operating systems, after the SVGA driver is installed, you are prompted to reboot to use this new driver.

The wizard finishes installing VMware Tools.

- 4 Reboot the virtual machine if necessary.

To change the default configuration options, see [“Open the VMware Tools Control Panel”](#) on page 121.

Configure the Video Driver on Older Versions of Windows

If you are installing VMware Tools in a virtual machine that has a Windows NT, Windows Me, Windows 98, or Windows 95 operating system, you might need to configure the video driver manually. When you click **Finish** in the VMware Tools installation wizard, a message appears indicating that VMware Tools failed to install the SVGA driver appears.

A Notebook window, the Display Properties/Settings dialog box, and a message box prompting you to reboot the machine.

To configure the video driver on older versions of Windows

- 1 In the message box that prompts you to reboot, click **No**.

If you click **Yes**, after the virtual machine reboots, run the VMware Tools installer again (choose **VM > Install VMware Tools**). Select the **Repair** option. The **Repair** option allows the Notebook window to appear again so that the installer can access the SVGA driver.

- 2 Follow the instructions in the Notebook file.

The instructions are specific to each operating system. They provide steps for selecting the VMware SVGA driver, usually in the Display Properties/Settings dialog box, and installing it from the VMware Tools ISO image.

The English version of the instructions from the Notebook file are reprinted in Knowledge Base article 1001819 at the VMware Web site.

Automate the Installation of VMware Tools in a Windows Guest

If you are installing VMware Tools in a number of Windows virtual machines, you can automate its installation. This silent installation feature uses the Microsoft Windows Installer runtime engine.

Make sure the Microsoft Windows Installer runtime engine version 2.0 or higher is installed in the guest operating system.

Version 2.0 or higher is included with newer versions of Windows. If you are installing VMware Tools in older Windows guest operating systems, check the version of the %WINDIR%\system32\msiexec.exe file.

If the file version is not 2.0 or higher, upgrade the engine by running `instmsiw.exe` (`instmsia.exe` for Windows 95 or Windows 98 guests), which is included with the VMware Tools installer.

For more information about using the Microsoft Windows Installer, including command-line options, go to the Windows Installer page on the MSDN Web site.

To automate the installation of VMware Tools in a Windows guest

- 1 Make sure the virtual machine's CD-ROM drive is connected to the VMware Tools ISO image and that it is configured to connect whenever you power on the virtual machine:
 - a Select the virtual machine and choose **VM > Settings > Hardware > CD-ROM**.
 - b In the **Device status** section, select the **Connect at Power On** check box.
 - c In the **Connection** section, select **Use ISO image** and browse to the `windows.iso` file, located in the directory where you installed Workstation.
 - d Click **OK**.
- 2 (Optional) In the guest operating system, suppress prompts about installing unsigned drivers.

If you are installing VMware Tools from a beta or RC (release candidate) version of Workstation, you are asked to confirm the installation of unsigned drivers. Follow these steps to suppress these confirmation prompts.

For all Windows systems except Windows Vista:

- a On the virtual machine's desktop or **Start** menu, right-click **My Computer** and choose **Properties**.
- b Click the **Hardware** tab and click **Driver Signing**.

The Driver Signing dialog box appears.

- c Click **Ignore**, click **OK**, and click **OK** in the second dialog box.

For Windows Vista:

- a On the **Start** menu, right-click **Computer** and choose **Properties**.
- b Click **Advanced system settings > Hardware > Windows Update driver settings**.
- c Click **Never check for drivers when I connect a new device**, click **OK**, and click **OK** in the second dialog box.

- 3 Open a command prompt and use the following command to install some or all of the VMware Tools components:

```
msiexec -i "D:\VMware Tools.msi" ADDLOCAL=ALL [REMOVE=<component>] /qn
```

In this command, you can optionally use **REMOVE=<component>** if you do not want to install a particular component.

Valid Component Values	Description
Toolbox	VMware Tools control panel and its utilities. Excluding this feature prevents you from using VMware Tools in the guest operating system. VMware does not recommend excluding this feature.
Drivers	<p>Includes the SVGA, mouse, BusLogic, and vmxnet drivers.</p> <ul style="list-style-type: none"> ■ SVGA – VMware SVGA driver. Excluding this feature limits the display capabilities of your virtual machine. ■ Mouse – VMware mouse driver. Excluding this feature decreases mouse performance in your virtual machine. ■ BusLogic – VMware BusLogic driver. If your virtual machine is configured to use the LSI Logic driver, you might want to remove this feature. ■ VMXNet – VMware vmxnet networking driver.

Valid Component Values	Description
MemCtl	VMware memory control driver. Use this driver if you plan to use this virtual machine with VMware ESX Server. Excluding this feature hinders the memory management capabilities of the virtual machine running on an VMware ESX Server system.
Hgfs	VMware shared folders driver. Use this driver if you plan to use this virtual machine with VMware Workstation. Excluding this feature prevents you from sharing a folder between your virtual machine and the Workstation host.

For example, to install everything but the shared folders driver, type the following on the command line:

```
msiexec -i "D:\VMware Tools.msi" ADDLOCAL=ALL REMOVE=Hgfs /qn
```

The SVGA, Mouse, BusLogic, vmxnet, and MemCtl features are children of the Drivers feature. This means that the following command skips installation of the SVGA, mouse, BusLogic, vmxnet, and MemCtl drivers:

```
msiexec -i "D:\VMware Tools.msi" ADDLOCAL=ALL REMOVE=Drivers /qn
```

To include a feature, use it with the ADDLOCAL option. To exclude a feature, use it with the REMOVE option.

Install VMware Tools on a Linux Guest Within X by Using the RPM Installer

You can use a graphical user interface to install VMware Tools in a Linux guest. For information about how to install VMware Tool from the command line, see [“Install VMware Tools from the Command Line with the Tar or RPM Installer”](#) on page 111.

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools on a Linux Guest Within X by Using the RPM Installer

- 1 On the host, from the menu bar, choose **VM > Install VMware Tools**.

The guest operating system mounts the VMware Tools installation virtual CD. A window manager displaying two files might appear. One file is for the RPM installer and one is for the tar installer. Alternatively, a VMware Tools CD icon might appear on the desktop.

- 2 Do one of the following:

- If you see a **VMware Tools CD** icon on the desktop, double-click it, and after it opens, double-click the RPM installer in the root of the CD-ROM.
- If you see a file manager window, double-click the RPM installer file.

In some Linux distributions, the **VMware Tools CD** icon might fail to appear. In this case, install VMware Tools from the command line.

- 3 When prompted, enter the root password and click **OK**.

The installer prepares the packages.

- 4 Click **Continue** when the installer presents a dialog box that shows **Completed System Preparation**.

A dialog box appears with a progress bar. When the installer is done no confirmation window or finish button appears, but VMware Tools is installed.

- 5 In an X terminal, as root (**su -**), run the following file to configure VMware Tools:

```
vmware-config-tools.pl
```

Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value.

- 6 Exit from the root account.

```
exit
```

- 7 In an X terminal, to start the VMware Tools control panel, enter the following command:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see [“Open the VMware Tools Control Panel”](#) on page 121.

Install VMware Tools from the Command Line with the Tar or RPM Installer

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools from the command line with the tar or RPM installer

- 1 On the host, choose **VM > Install VMware Tools**.
- 2 On the guest, log in as root (**su -**).
- 3 If necessary, mount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

mount /dev/cdrom /mnt/cdrom

Some Linux distributions automatically mount CD-ROMs. If your distribution uses automounting, you can skip this step.

Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom` or if the mount point for a CD-ROM is not `/mnt/cdrom`, modify the command to reflect the conventions used by your distribution.

- 4 Change to a working directory by entering a command such as the following:

cd /tmp

- 5 If a previous installation exists, delete the previous `vmware-tools-distrib` directory before installing.

The location of this directory depends on where you placed it during the previous installation. Often it is placed in:

`/tmp/vmware-tools-distrib`

- 6 Run the installer and unmount the CD-ROM image.

Depending on whether you are using the tar installer or the RPM installer, do one of the following:

- For the tar installer, at the command prompt, enter:

tar xzpf /mnt/cdrom/VMwareTools-5.0.0-`<xxxx>`.tar.gz umount /dev/cdrom

Where `<xxxx>` is the build number of the Workstation release.

- For the RPM installer, at the command prompt, enter:

rpm -Uvh /mnt/cdrom/VMwareTools-5.0.0-`<xxxx>`.i386.rpm umount /dev/cdrom

Where `<xxxx>` is the build number of the Workstation release.

If your Linux distribution automatically mounted the CD-ROMs, you do not need to use the `umount` portion of the command.

If you attempt to install an RPM installation over a tar installation or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

- 7 Configure VMware Tools.

Depending on whether you are using the tar installer or the RPM installer, do one of the following:

- For the tar installer, enter the following commands to run the installer:


```
cd vmware-tools-distrib  
./vmware-install.pl
```

Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value. The configuration file, `vmware-config-tools.pl`, runs after the installer file finishes running.

- For the RPM installer, enter the following command to run the configuration file:

```
vmware-config-tools.pl
```

Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value.

- 8 Log out of the root account.

```
exit
```

- 9 Start your graphical environment.

- 10 In an X terminal, enter the following command to start the VMware Tools control panel:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see [“Open the VMware Tools Control Panel”](#) on page 121.

Install VMware Tools in a Solaris Guest

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a Solaris guest

- 1 On the host, choose **VM > Install VMware Tools**.
- 2 On the guest, log in as root (**su -**).
- 3 If necessary, mount the VMware Tools virtual CD-ROM image.

Usually, the Solaris volume manager `vold` mounts the CD-ROM under `/cdrom/vmwaretools`. If the CD-ROM is not mounted, restart the volume manager using the following commands:

```
/etc/init.d/volmgt stop  
/etc/init.d/volmgt start
```

- 4 After the CD-ROM is mounted, change to a working directory (for example, `/tmp`) and extract VMware Tools by entering the following commands:

```
cd /tmp
gunzip -c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf -
```

- 5 Run the VMware Tools tar installer:

```
cd vmware-tools-distrib
./vmware-install.pl
```

Respond to the configuration questions on the screen. Press Enter to accept the default value.

- 6 Log out of the root account:

```
exit
```

- 7 Start your graphical environment.

- 8 In an X terminal, enter the following command to start the VMware Tools control panel:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see [“Open the VMware Tools Control Panel”](#) on page 121.

Install VMware Tools in a FreeBSD Guest

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a FreeBSD guest

- 1 On the host, choose **VM > Install VMware Tools**.
- 2 Make sure the guest operating system is running in text mode.
You cannot install VMware Tools while X is running.
- 3 On the guest, log in as root (**su -**).
- 4 If necessary, mount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

```
mount /cdrom
```

Some FreeBSD distributions automatically mount CD-ROMs. If your distribution uses automounting, skip this step.

- 5 Change to a working directory by entering a command such as the following:

```
cd /tmp
```

- 6 Untar the VMware Tools tar file:

```
tar xzpf /cdrom/vmware-freebsd-tools.tar.gz
```

- 7 If necessary, unmount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

```
umount /cdrom
```

If your distribution uses automounting, skip this step.

- 8 Run the VMware Tools installer:

```
cd vmware-tools-distrib  
./vmware-install.pl
```

- 9 Log out of the root account:

```
exit
```

- 10 Start your graphical environment.

- 11 In an X terminal, enter the following command to start the VMware Tools control panel:

```
vmware-toolbox &
```

In minimal installations of the FreeBSD 4.5 guest operating system, sometimes VMware Tools does not start. See [“Install the Missing FreeBSD Library”](#) on page 115.

To change the default VMware Tools configuration options, see [“Open the VMware Tools Control Panel”](#) on page 121.

Install the Missing FreeBSD Library

If VMware Tools does not start after you install it, you might need to install a library that is missing because you do not have a full installation of FreeBSD 4.5.

Before you begin, make sure you have the FreeBSD 4.5 installation CD or access to the ISO image file.

To install the missing FreeBSD library

- 1 Reboot the guest operating system.
- 2 On the guest, in an X terminal, enter the following command to start the VMware Tools control panel:

```
vmware-toolbox &
```

If the following error message appears, the required library was not installed:

```
Shared object 'libc.so.3' not found.
```

- 3 Insert and mount the FreeBSD 4.5 installation CD or access the ISO image file.
- 4 Change directories and run the installation script:

```
cd /cdrom/compat3x  
./install.sh
```

Install VMware Tools in a NetWare Virtual Machine

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a NetWare virtual machine

- 1 On the host, choose **VM > Install VMware Tools**.
- 2 On the guest, load the CD-ROM driver so the CD-ROM device mounts the ISO image as a volume by doing one of the following:

- For a NetWare 6.5 virtual machine in the system console, enter:

```
LOAD CDDVD
```

- For a NetWare 6.0 or NetWare 5.1 virtual machine, in the system console, enter:

```
LOAD CD9660.NSS
```

- For a NetWare 4.2 virtual machine, in the system console, enter:

```
load cdrom
```

Mount the VMware Tools CD-ROM image by entering:

```
cd mount vmwtools
```

- 3 In the system console, enter one of the following:

- For NetWare 5.1, 6.0, or 6.5:

```
vmwtools:\setup.ncf
```

- For NetWare 4.2:

```
vmwtools:\setup
```

When the installation finishes, the message **VMware Tools for NetWare are now running** appears in the Logger Screen (NetWare 6.5 and NetWare 6.0 guests) or the Console Screen (NetWare 4.2 and 5.1 guests).

- 4 If you have a NetWare 4.2 guest, restart the guest operating system, as follows:

- a To shut down the system, in the system console, enter:

down

- b To restart the guest operating system, in the system console, enter:

restart server

- 5 Make sure the VMware Tools virtual CD-ROM image (`netware.iso`) is not attached to the virtual machine.

If it is attached, disconnect it. Right-click the CD-ROM icon in the status bar of the console window and choose **Disconnect**.

Start vmware-user Manually If You Do Not Use a Session Manager on UNIX

One of the executables used by VMware Tools in UNIX guests is `vmware-user`. This program implements the fit-guest-to-window feature, among other features.

Normally on Linux, the VMware Tools service (`vmware-guestd`) starts and stops `vmware-user`. On Solaris, `vmware-user` is started automatically after you configure VMware Tools and then log out of the desktop environment and log back in.

However, if you run an X session without a session manager (for example, by using `startx` and getting a desktop and not using `xdm`, `kdm`, or `gdm`), `vmware-guestd` does not start and stop `vmware-user`, and you must do it manually.

To start vmware-user manually if you do not use a session manager

Add `vmware-user` to the appropriate X startup script.

The `vmware-user` program is located in the directory where you selected to install binary programs, which defaults to `/usr/bin`. The startup script that needs to be modified depends on your particular system.

VMware Tools Update Process

Because VMware Tools installers (ISO images) are installed with VMware Workstation, when you update to a new version of Workstation, a check is performed to determine if a new version of VMware Tools is available. Although you can set Workstation to check regularly for Workstation updates, the guest operating system checks for VMware Tools updates only when you power on a virtual machine. It compares its version of VMware Tools against the version that is installed on the host.

For VMware Tools updates on Linux and Windows guests, you can set the guest to update automatically or you can perform a manual update. On other guests, you must manually update.

When you update VMware Tools, any changes you made to the default scripts are overwritten. Any custom scripts you created remain untouched, but do not benefit from any underlying changes that enhance the default scripts.

How Automatic Updates Occur

On Windows and Linux guest systems, you can set VMware Tools to update itself when the virtual machine is powered on. The status bar displays the message **Installing VMware Tools** . . . when an update is in progress. After the update is complete, if you are logged in to a Windows guest, a restart prompt appears for 30 seconds. If you are not logged in, the operating system restarts without prompting.

Automatic updates work for versions of VMware Tools included in Workstation 5.5 and above (build 29772 and above). Automatic updates do not work for versions of VMware Tools included in virtual machines created with VMware Server 1.x.

An auto-update check is performed as part of the boot sequence when you power on a virtual machine. If the virtual machine was suspended and you resume it or restore it to a snapshot during the boot sequence before this check occurs, the automatic update occurs as planned.

If you resume the virtual machine or restore it to a snapshot after the auto-update check occurs, the automatic update does not occur.

For more information about automatic updates, see [“Use Global Settings to Update VMware Tools Automatically”](#) on page 119 and [“Set Autoupdate Options for Each Virtual Machine”](#) on page 119.

How You Are Notified to Do a Manual Update

On Windows and Linux guests, you can specify that no automatic update should occur. On other operating systems, automatic updates are not possible. In these cases, perform a manual update.

The status bar of the guest system displays a message when a new version is available. To install the update, use the same procedure that you used for installing VMware Tools the first time.

On Windows, you can alternatively open the VMware Tools control panel (double-click the **VMware Tools** icon in the notification area of the taskbar), and on the **Options** tab, click **Upgrade**.

Use Global Settings to Update VMware Tools Automatically

To automatically update VMware Tools for most or all Windows or Linux guests when the virtual machine starts, configure the global preference first and then configure the per-virtual-machine update option to use that global preference.

To use global settings to update VMware Tools automatically

- 1 Start Workstation.
If you use a UNIX host, become root (**su -**) before starting Workstation. On UNIX systems, nonroot users are not allowed to modify the preference setting for VMware Tools updates.
- 2 Choose **Edit > Preferences** and click the **Tools** tab.
- 3 Select the check box on this tab and click **OK**.
- 4 For each of your virtual machines, do the following:
 - a Select the virtual machine.
The virtual machine can be either powered on or powered off.
 - b Choose **VM > Settings**.
The virtual machine settings editor opens.
 - c Click the **Options** tab and select **Tools**.
 - d Select **Use global settings** from **Edit > Preferences > Tools** and click **OK**.

Set Autoupdate Options for Each Virtual Machine

Use this procedure to override global settings for automatically updating VMware Tools on Linux and Windows guests.

To set autoupdate options for each virtual machine

- 1 Select the Linux or Windows virtual machine.
The virtual machine can be either powered on or powered off.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 Click the **Options** tab and select **Tools**.
- 4 Select an update option and click **OK**.
For more information about the options, click **Help**.

Update VMware Tools in Older Windows Virtual Machines

When a Microsoft installer performs an update, it updates only the components that it finds already installed. It does not add new components. If you update VMware Tools in a Windows virtual machine that was created with Workstation 5.x, some new components are not installed. Specifically, the Workstation 6 component for file sharing and dragging and dropping files is not installed.

To get the new components, you must uninstall the old version of VMware Tools and install the new version of VMware Tools.

To update VMware Tools in older Windows virtual machines

- 1 To uninstall the old version of VMware Tools, use the **Add/Remove Programs** item in the guest's Control Panel.
- 2 To install the new version of VMware Tools, see [“Installing VMware Tools”](#) on page 105.

Uninstall VMware Tools

Occasionally, an update of VMware Tools is incomplete. You can usually solve the problem by uninstalling VMware Tools and then reinstalling.

To uninstall VMware Tools

Depending on the guest operating system, do one of the following:

- On a Windows guest, use the guest operating system's **Add/Remove Programs** item to remove VMware Tools.
- On any UNIX guest, log on as root (**su -**) and enter the appropriate command:
vmware-uninstall-tools.pl
- On a Linux guest that has VMware Tools installed by using an RPM installer, you can uninstall by using the following command:
rpm -e VMwareTools

Repair or Change Installed Modules

If features like enhanced file sharing do not work after a VMware Tools update, you might need to change or repair installed modules. Be sure to follow these steps. Do not the guest's **Add/Remove Programs** item in the Windows Control Panel.

To repair or change installed modules

- 1 In Workstation, select the virtual machine and choose **VM > Install VMware Tools**.

Because the latest version of VMware Tools is installed, a Change wizard appears.

- 2 Click **Change** to repair or modify which components of VMware Tools are installed.

- 3 Click **Modify** to specify which modules are installed.

Occasionally, some new modules are not installed during an update. You can manually install new modules by using the **Modify** option.

- 4 Do one of the following:

- If the new modules you want are not listed as installed, continue with the **Modify** option to install them.
- If the problem modules are listed as installed, click **Back** and use the **Repair** option.

- 5 Complete the rest of the pages of the wizard.

If features still do not work, uninstall VMware Tools and reinstall.

Open the VMware Tools Control Panel

Use the VMware Tools control panel to modify VMware Tools configuration settings, shrink virtual disks, and connect and disconnect virtual devices.

Before you begin, make sure VMware Tools is installed in the guest operating system.

On Windows Vista guests, log in to the operating system as an Administrator user.

To open the VMware Tools control panel

Do one of the following:

- On Windows guests, double-click **VMware Tools** icon in the notification area of the guest's Windows taskbar.

If you cannot find the **VMware Tools** icon in the notification area, use the guest's Windows Control Panel to display it.

- On Linux, FreeBSD, and Solaris guests, open a terminal window and enter the command:

```
/usr/bin/vmware-toolbox &
```

- On NetWare guests, do one of the following:
 - In a NetWare 5.1 or higher guest, choose **Novell > Settings > VMware Tools for NetWare**.
 - In a NetWare 4.2 guest, use VMware Tools commands in the system console. The VMware Tools program is called `vmwtool`.

Use the Windows Control Panel to Display the VMware Tools Taskbar Icon

If VMware Tools is installed in a Windows guest operating system but the **VMware Tools** icon does not appear in the notification area of the Windows taskbar, you can use the Windows Control Panel to display it.

To display the VMware Tools taskbar icon

- 1 Go to **Start > Control Panel**.
- 2 Double-click the **VMware Tools** icon.
- 3 On the **Options** tab, select **Show VMware Tools in the taskbar** and click **Apply**.

Options Tab Settings

The **Options** tab of the VMware Tools control panel provides the following options:

- **Time synchronization between the virtual machine and the host operating system** – Synchronizes the time in the guest with the time on the host if the clock in the guest lags behind the time set on the host. If you use this option, disable all other time synchronization mechanisms. For example, some guests might have NTP or CMOS clock synchronization turned on by default. VMware recommends that you use the VMware Tools time synchronization mechanism.
- **Show VMware Tools in the taskbar** – (Windows guests only) Displays the **VMware Tools** icon in the notification area of the taskbar. The icon indicates whether VMware Tools is running and whether an update is available.
- **Notify if upgrade is available** – (Windows guests only) Displays the **VMware Tools** icon with a yellow caution icon when an update is available.
- **Upgrade** button – (Windows guests only) Becomes enabled when an update is available. Clicking this button has the same effect as choosing **VM > Install VMware Tools** from the Workstation menu bar.

Additional Time Synchronization Options

If the guest is set to a later time than the host, you can use a command-line option to synchronize time. See [“Use the VMware Tools Command-Line Interface”](#) on page 133.

Under some circumstances, the virtual machine might synchronize time with the host even though this item is not selected. To disable time synchronization completely, you can edit the virtual machine’s configuration (.vmx) file and set the time sync options to FALSE. See [“Disable Time Synchronization by Editing the Virtual Machine Configuration File”](#) on page 123.

Disable Time Synchronization by Editing the Virtual Machine Configuration File

Under some circumstances, the virtual machine might synchronize time with the host even though you used the VMware Tools control panel (**Options** tab) to disable time synchronization. If you see this problem, disable time synchronization by editing the virtual machine configuration file.

You can follow these steps to keep a fictitious time in your guest, so that the guest is never synchronized with the host.

You can alternatively use the VMware Tools command-line interface to set these time synchronization options. If you use this command-line interface, you do not need to power off the virtual machine. See [“Use the VMware Tools Command-Line Interface”](#) on page 133.

To disable time synchronization by editing the virtual machine configuration file

- 1 Power off the virtual machine.
- 2 Open the virtual machine’s configuration file (.vmx) in a text editor and set the following options to FALSE.

Option Name	Synchronization Occurs During the Following Event
time.synchronize.tools.enable	Powering on a virtual machine. Controls whether toggling the <code>syncTime</code> option to TRUE causes an immediate, one-time synchronization to occur.
tools.syncTime	Powering on a virtual machine.
time.synchronize.restore	Reverting to a snapshot.
time.synchronize.resume.disk	Resuming a suspended virtual machine.

Option Name	Synchronization Occurs During the Following Event
time.synchronize.continue	Taking a snapshot.
time.synchronize.shrink	Shrinking a virtual disk.

- 3 Save and close the file.

Devices Tab Settings

The **Devices** tab of the VMware Tools control panel provides options for enabling and connecting to removable devices such as floppy drives, DVD/CD-ROM drives, ISO images, USB devices, sound adapters, and Ethernet adapters.

The controls for connecting and disconnecting devices might not be available, depending on whether your system administrator enabled them.

You might not see a particular Ethernet adapter listed that should appear in the list. If this happens, edit the virtual machine settings to remove all Ethernet adapters from the list and then add them back to the list.

Besides using the VMware Tools control panel to connect or disconnect a device, you can right-click the device icon in the status bar of the virtual machine window. See [“Use Removable Devices in a Virtual Machine”](#) on page 166.

Scripts Tab Settings

From the **Scripts** tab of the VMware Tools control panel, you can edit, disable, or run scripts that help automate guest operating system operations when you change the virtual machine's power state. .

From this tab, you can also specify the location of custom scripts for the **Suspend**, **Resume**, **Power On**, **Power Off**, and **Reset** buttons.

On most guest operating systems, if VMware Tools is installed and if you configure a virtual machine's power controls to use the guest options, one or more default scripts run on the guest whenever you change the power state of the virtual machine.

For example, if you use the virtual machine settings editor (choose **VM > Settings > Options > Power**) and set the **Power Off** control to use **Shutdown Guest**, then the `poweroff-vm-default` script runs when you click the **Power Off** button in the Workstation toolbar. This script causes the guest operating system to shut down gracefully.

Scripts can be run on most guest operating systems, but not on Windows 95, NetWare, and FreeBSD guests. See [“Run or Disable a Script”](#) on page 130.

Shared Folders Tab Information

The **Shared Folder** tab of the VMware Tools control panel tab is available only on newer Windows guests and only when shared folders are enabled. It provides information on how to access your shared folders on the host, so you can share files between the host and guest.

With a shared folder, you can share files between two virtual machines and between a virtual machine and the host operating system, even if one has a Windows operating system and the other has Linux or Solaris.

Although the **Shared Folders** tab does not appear in Linux or Solaris guests, you can share folders with Linux and Solaris guests. See [“Set Up Shared Folders”](#) on page 178.

The shared folders feature works only when the virtual machine is running under newer versions of some VMware products and only when shared folders are enabled for the virtual machine. Shared folders are not supported with Windows 95, Windows 98, Windows Me, and FreeBSD guest operating systems.

Shrink Tab Settings

The **Shrink** tab of the VMware Tools control panel provides options for reclaiming unused space in a virtual disk. If your virtual machine cannot be shrunk, this tab displays information explaining why you cannot shrink your virtual disks.

Shrinking a disk is a two-step process: a preparation step and the shrink step. In the first step, VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. This step takes place in the guest operating system.

The shrink process is the second step, and it takes place outside the virtual machine. The VMware application reduces the size of the disk based on the disk space reclaimed during the preparation step. If the disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive.

On UNIX guests, run VMware Tools as the root user (**su -**) to shrink virtual disks. If you shrink the virtual disk as a nonroot user, you cannot prepare to shrink the parts of the virtual disk that require root-level permissions.

See [“Shrink a Virtual Disk”](#) on page 218.

About Tab

The **About** tab displays version (build number) and copyright information. In Windows guests, this tab also shows the status of the VMware Tools service.

Configure VMware Tools in a NetWare Guest

In a NetWare virtual machine, using the system console, you can configure certain virtual machine options such as time synchronization, CPU idling, and device configuration with VMware Tools. The VMware Tools command-line program is called `vmwtool`.

To configure VMware Tools in a NetWare Guest

- 1 Open a terminal window (system console) in the NetWare guest.
- 2 Enter a command that uses the following format:

`vmwtool <command>`

`<command>` is one of the commands listed in the following table.

vmwtool Command	Description
help	Displays a summary of VMware Tools commands and options in a NetWare guest.
partitonlist	Displays a list of all disk partitions in the virtual disk and whether or not a partition can be shrunk.
shrink [<partition>]	Shrinks the listed partitions. If no partitions are specified, all partitions in the virtual disk are shrunk. The status of the shrink process appears at the bottom of the system console.
devicelist	Lists each removable device in the virtual machine, its device ID, and whether the device is enabled or disabled. Removable devices include the virtual network adapter, CD-ROM, and floppy drives.
disabledevice [<device name>]	Disables the specified device or devices in the virtual machine. If no device is specified, all removable devices in the virtual machine are disabled.
enabledevice [<device name>]	Enables the specified device or devices in the virtual machine. If no device is specified, all removable devices in the virtual machine are enabled.

vmwtool Command	Description
<code>synctime [on off]</code>	Lets you turn on or off synchronization of time in the guest operating system with time on the host operating system. By default, time synchronization is turned off. Use this command without any options to view the current time synchronization status.
<code>idle [on off]</code>	Lets you turn the CPU idler on or off. By default, the idler is turned on. The CPU idler program is included in VMware Tools for NetWare guests. The idler program is needed because NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy.

Customizations to VMware Tools

Customizations include modifying or writing scripts that run when a virtual machine's power state changes, executing commands when you shut down or restart a UNIX guest, and passing commands in strings that run in startup scripts.

How VMware Tools Scripts Affect Power States

When VMware Tools is installed, if you configure a virtual machine's power controls to use the guest, or soft, power options, one or more default scripts run on the guest whenever you change the power state of the virtual machine. You change the power state by using menu commands or by clicking the **Suspend**, **Resume**, **Power On**, and **Power Off** buttons.

What the default scripts do depends in part on the guest operating system:

- On most Microsoft Windows guests, but not windows NT and Windows Me, the default script executed when you suspend a virtual machine releases the IP address of the virtual machine. The default script executed when you resume a virtual machine renews the IP address of the virtual machine (this affects only virtual machines configured to use DHCP). Scripts cannot be run on Windows 95 guests.

In Windows guests, the default scripts are located in the Program Files\VMware\VMware Tools folder.

- On most UNIX guests, the default script executed when you suspend a virtual machine stops networking for the virtual machine. The default script executed

when you resume a virtual machine starts networking for the virtual machine. Scripts cannot be run on NetWare and FreeBSD guests.

On UNIX, the default scripts are located in the `/etc/vmware-tools` directory.

You can create your own scripts and use them instead of the default scripts shown in [Table 6-1](#).

Table 6-1. Default VMware Tools Scripts

Script Name	Description
<code>poweroff-vm-default</code>	<p>If you configured the power-off operation to shut down the guest, this script runs when the virtual machine is being powered off.</p> <p>If you configured the reset operation to restart the guest, this script runs when the virtual machine is being reset.</p> <p>This script has no effect on networking for the virtual machine.</p>
<code>poweron-vm-default</code>	<p>If you configured the power-on operation to start the guest, this script runs when the virtual machine is being powered on rather than resumed.</p> <p>If you configured the reset operation to restart the guest, this script runs after virtual machine restarts.</p> <p>This script has no effect on networking for the virtual machine.</p>
<code>resume-vm-default</code>	<p>If you configured the power-on operation to start the guest, or the reset operation to restart the guest, this script runs when the virtual machine is resumed after it was suspended.</p> <p>On Windows guests, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine.</p> <p>On Linux, FreeBSD, and Solaris guests, this script starts networking for the virtual machine.</p>
<code>suspend-vm-default</code>	<p>If you configured the suspend operation to suspend the guest, this script runs when the virtual machine is being suspended.</p> <p>On Windows guests, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine.</p> <p>On Linux, FreeBSD, and Solaris guests, this script stops networking for the virtual machine.</p>

Create Scripts to Override Default VMware Tools Scripts

Use the instructions in this topic to override the default VMware Tools scripts and create your own scripts to control power state changes.

Scripts are run by the VMware Tools daemon (`VMwareService.exe` on Windows and `vmware-guestd` on UNIX). Because `vmware-guestd` is run as root on UNIX and as System on Windows, the scripts are run in a separate session from the logged-in user's session. The VMware Tools daemon has no knowledge of desktop sessions, which

means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

Before creating custom scripts, make sure that the following conditions are met in the guest operating system:

- The virtual machine is using the latest version of VMware Tools.
- The VMware Tools service is running in the virtual machine.
- Depending on the operation the script performs, the virtual machine has a virtual network adapter connected. If not, the power operation fails.
- (UNIX guests only) To edit a script by using the **Edit** button on the **Scripts** tab, `xterm` and `vi` must be installed in the guest operating system and must be in your `PATH`. You must be a root user to edit the script.

To create custom VMware Tools scripts

- 1 Determine whether you want to create your custom script by making changes to the default script and saving it to a new location.

In Windows guests, the default scripts are located in the `Program Files\VMware\VMware Tools` folder.

On UNIX, the default scripts are located in the `/etc/vmware-tools` directory.

- 2 Modify the default script and save it with a different name or write a different script.

On Windows guests, if you write a new script, create the script as a batch file. For UNIX, create the script in any executable format (such as shell or Perl scripts).

You can also use the **Edit** button on the **Scripts** tab of the VMware Tools control panel to edit a custom script. You can also edit scripts manually using any text editor.

- 3 Associate each custom script with its particular power operation:
 - a On the **Scripts** tab of the VMware Tools control panel, select the appropriate script event.
 - b Select the **Use Script** check box, select **Custom script**, and use the **Browse** button to point to the script you want to use.
 - c Click **OK**.

When you reinstall VMware Tools after you update the Workstation software, any changes you made to the default scripts are overwritten. Any custom scripts you

created remain untouched, but do not benefit from any underlying changes that enhance the default scripts.

Run or Disable a Script

If you are creating a custom script, run the script before associating it with a power operation.

To run or disable a script

- 1 On the **Scripts** tab of the VMware Tools control panel, select the appropriate script event.
- 2 Do one of the following:

- To disable the script, clear the **Use Script** check box and click **OK**.

Default scripts for suspending and resuming work together. If you disable the script of one of these actions, disable the script for the other action as well.

- To run a script immediately, click **Run Now**.

You can successfully run a script by clicking the **Run Now** button in the VMware Tools control panel, but this same script can fail when run as part of a Workstation power operation. This is because scripts run by clicking **Run Now** are run as the logged-in user and have a different working directory than when scripts are run by the VMware Tools daemon during a power operation.

Execute Commands After You Power Off or Reset a Virtual Machine

In a Linux, Solaris, or FreeBSD guest, you can use the VMware Tools service to execute specific commands when you shut down or restart the guest operating system. This is in addition to any script that you specified to run when you shut down the guest operating system.

- 1 Use a text editor to open the following file:
`/etc/vmware-tools/tools.conf`
- 2 Add one or both of the following commands to the file:

- **halt-command** = <command>

<command> is the command to execute when you shut down the guest operating system.

- **reboot-command** = <command>

<command> is the command to execute when you restart the guest operating system.

Passing a String from the Host to the Guest at Startup

To pass a string from the host to the guest at startup, you pass the string from your virtual machine's configuration file in the host to the guest operating system when you power on the virtual machine.

You can pass items like the Windows system ID (SID), a machine name, or an IP address. Inside the guest operating system startup script, you can have the service retrieve this string. The string can then be used in another script to set your virtual machine's system ID, machine name, or IP address.

Use this strategy, for example, to make copies of the same configuration file, add a different string to each (either in the configuration file itself or at the command line), and use these variations of the same configuration file to launch the same virtual disk in nonpersistent mode multiple times in a training or testing environment.

Passing a string is also useful when you want to deploy virtual machines on a network using a common configuration file while providing each machine with its own unique identity.

You can pass strings to a virtual machine's guest operating system in one of two ways: placing the string in the virtual machine's configuration file or passing the string to the guest from the command line.

Use this feature only if you have a good understanding of a scripting language (for example, Perl or NetShell) and know how to modify system startup scripts.

String in a Configuration File

Place a string in the virtual machine's configuration file (.vmx file) by setting the string to the `machine.id` parameter. For example, you can set this string:

```
machine.id = "Hello World."
```

Following is an example of portions of two configuration files that point to the same virtual disk. Each configuration file contains its own unique string set for the `machine.id` parameter.

`config_file_1.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_first_vm"
```

`config_file_2.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_second_vm"
```

To prevent a string from being passed from the host to the guest through the service, set the following line in your virtual machine's configuration file:

```
isolation.tools.getMachineID.disable = "TRUE"
```

String in a Startup Command

Rather than setting the `machine.id` parameter in the configuration file, you can pass the string to the guest operating system from the command line when you power on the virtual machine. Following is an example of such a startup command (entered on one line):

```
"C:\Program Files\VMware\VMware Workstation\vmware -s
'machine.id=Hello World'
C:\Virtual Machines\win2000\win2000.vmx"
```

Use this method to deploy virtual machines on a network using a common configuration file while providing each machine with its own unique identity.

Launch each virtual machine with the **vmware -s** command. Each virtual machine disk file must be copied into its own directory if it shares its filename with another virtual machine disk file.

On a Linux host, the machine ID passed on the command line takes precedence and is passed to the guest operating system if the following conditions are met:

- A virtual machine ID is specified in the virtual machine's configuration (.vmx) file which is used to open the virtual machine.
- You specify a machine ID on the command line.

Use a String in a Startup Script to Set a Name and IP Address

The following example uses a Windows host to illustrate how you can use the service to retrieve a string containing what becomes the virtual machine's machine name and IP address. In this example, W2K-VM is the machine name and 148.30.16.24 is the IP address.

To use a string in a startup script to set a name and IP address

- 1 Define the string by using one of the following methods:

- On the host machine, add the following line to your virtual machine's configuration file (.vmx file):

```
machine.id = "W2K-VM 148.30.16.24"
```

Open the virtual machine using this configuration file.

- Open the virtual machine from the command line by entering the following on one line:

```
"C:\Program Files\VMware\VMware Workstation\vmware -s
'machine.id=W2K-VM 148.30.16.24' C:\Virtual
Machines\win2000\win2000.vmx"
```

- 2 Do one of the following to retrieve the string in the virtual machine:

- In a Windows guest, enter the following command to retrieve the string:

```
VMwareService --cmd machine.id.get
```

- In a Linux guest, in the operating system's startup script, add the following command before the network startup section. For example:

```
/usr/sbin/vmware-guestd --cmd 'machine.id.get'
```

The location of `vmware-guestd` depends on the directory you specify at the time of installation.

- 3 Further customize this startup script so that it uses the string the service retrieved during startup to set the virtual machine's network name to W2K-VM and its IP address to 148.30.16.24.
- 4 Place this string in the script before the command to start the network services.

If you're using a Windows 2000 guest operating system, for example, you can call the NetShell utility (`netsh`) and pass it the contents of the string, which uses the string accordingly. That is, it can set a new IP address for the virtual machine, if that is what was passed in the string originally.

Passing Information Between the Guest and Another Program

The VMware Tools service allows you to use VMware programmatic interfaces to manage virtual machines from your own independent programs and from existing frameworks developed by partners and third parties.

For more information about the VMware Infrastructure SDK, go to the VMware APIs and SDKs Documentation page of the VMware Web site.

Use the VMware Tools Command-Line Interface

The VMware Tools command-line interface you do the following:

- Configure time synchronization in your Linux guest operating system without running X.

- Use some special time synchronization options without power off the virtual machine and editing its configuration (.vmx) file.
- Configure VMware Tools options from the command line rather than from the VMware Tools control panel.

To use the VMware Tools command-line interface

- 1 On the guest operating system, change directories to the directory that contains the VMware Tools daemon.

Depending on the operating system, the name and default location of the daemon are as follows:

- On Microsoft Windows systems, the daemon is called `VMwareService.exe` and the location is:

`C:\Program Files\VMware\VMware Tools\VMwareService.exe`

- On UNIX systems, the daemon is called `vmware-guestd`. The location of `vmware-guestd` depends on the directory you specify at the time of installation. The default location is:

`/usr/sbin/vmware-guestd`

- 2 Use the `vmx.set_option` command to set the option.

Use the following syntax:

```
<daemon> --cmd "vmx.set_option <option> <old_val> <new_val>"
```

`<daemon>` is **vmware-guestd** on UNIX systems or **VMwareService.exe** on Windows systems.

`<option>` is one of the time synchronization options. See [“Options for the VMware Tools --cmd Command”](#) on page 135.

`<old_val>` and `<new_val>` are the old and new values, respectively. Use 0 to mean FALSE and 1 to mean TRUE.

Following is an example of setting time synchronization to TRUE on a Linux guest:

```
./vmware-guestd --cmd "vmx.set_option synctime 0 1"
```

When you use command-line options, the new settings are written into the virtual machine's configuration (.vmx) file.

For information about available commands other than the `--cmd` command, use the `--help` command-line command.

Options for the VMware Tools --cmd Command

Following are the options you can use as arguments to the `vmx.set_option` command-line command.

`synctime`

(Default is 0, which means FALSE) Controls whether the VMware Tools daemon periodically (every minute) checks whether the guest operating system's time is lagging behind the host's. If so, the guest's clock is moved forward to match the host's clock. If the guest's clock is ahead of the host's clock, the periodic time synchronization does not correct it.

Using the `synctime` command-line option is equivalent to using the time synchronization option on the **Options** tab of the VMware Toolbox, which sets a property called `tools.syncTime` in the virtual machine's configuration (`.vmx`) file.

`time.synchronize.tools.enable`

(Default is 1, which means TRUE) Controls whether toggling the `synctime` option to 1 causes an immediate, one-time synchronization to occur. Unlike the normal periodic time sync, which can move the guest clock only forward, this special time synchronization can move the guest clock either forward or backward.

`time.synchronize.tools.startup`

(Default is 1, which means TRUE) Controls whether the VMware Tools daemon conducts a single time synchronization when it starts up. This special time sync can be either forward or backward in time. The VMware Tools daemon starts whenever the guest operating system is booted. To keep a fictitious time in your guest so that the guest is never synchronized with the host, disable time synchronization altogether. See [“Disable Time Synchronization by Editing the Virtual Machine Configuration File”](#) on page 123.

BETA

Creating a Virtual Machine from a System Image or Another Virtual Machine

7

This chapter describes how to convert a physical machine, virtual machine, or system image to a VMware virtual machine. You can convert a virtual machine that was created by using a VMware product or a third-party product. This chapter includes the following topics:

- [“Conversion Process for Importing Virtual Machines from Other Formats”](#) on page 137
- [“VMware Converter Compared to the Conversion Wizard in Workstation”](#) on page 139
- [“Supported Source Machines”](#) on page 139
- [“Supported Destinations”](#) on page 144
- [“Conversion Impact on Settings”](#) on page 146
- [“Open a Third-Party Virtual Machine or System Image”](#) on page 147
- [“Import a Virtual Machine, Virtual Appliance, or System Image”](#) on page 148

Conversion Process for Importing Virtual Machines from Other Formats

On Windows hosts, Workstation 6.5 incorporates the Conversion wizard from the VMware Converter product. Using the Conversion wizard to perform a conversion to VMware virtual machines enables you to do the following:

- Avoid reinstalling operating systems and applications for system configurations you use often.

- Overcome legacy migration barriers. Certain legacy systems might be impossible to recreate through reinstallation.
- Convert a physical machine into a virtual machine.
- Use virtual machines or system images created with products from other companies such as Norton, Symantec, and StorageCraft.
- Convert virtual appliances. Supported file types include OVF and OVA.

Workstation provides two ways to convert a virtual machine or system image:

- Using the **File > Open** command converts and opens a virtual machine or system image quickly. Workstation uses default settings to make the conversion automatically, with no input required from you. The original Microsoft Virtual PC, Symantec Backup Exec System Recovery, StorageCraft ShadowProtect, or Acronis True Image (.vnc, .spf, .sv2i, or .tib) file is unchanged. The **File > Open** command creates a linked clone when it opens the file.

If you attempt to open a virtual machine or system image that is password protected, you are prompted to use the Conversion wizard.

- Using the **File > Import** command starts the Conversion wizard. It lets you specify the converted virtual machine's location, whether or not the converted virtual machine shares virtual disks with the original virtual machine or system image, and whether the converted virtual machine is to be compatible with Workstation 4.x, 5.x, or 6.0.x; ESX 2.x or 3.x; GSX Server 3.x; or VMware ACE 1.x or 2.

The wizard creates a completely new VMware virtual machine based on the input virtual machine or system image. The newly migrated VMware virtual machine retains the configuration of the original virtual machine or image.

The migration process can be nondestructive, so you can continue to use the original virtual machine with Microsoft Virtual PC, or the original system image with Symantec Backup Exec System Recovery. However, to run a new VMware virtual machine on the same network as the original Virtual PC virtual machine, you must modify the network name and IP address on one of the virtual machines so the original and new virtual machines can coexist.

For Microsoft Virtual PC and Microsoft Virtual Server virtual machines, you have the option of sharing the source virtual hard disk (.vhd) files. This means that the VMware virtual machine can write directly to the original .vhd files instead of VMware virtual hard disk (.vmdk) files.

VMware Converter Compared to the Conversion Wizard in Workstation

Workstation 6.5 incorporates the Conversion wizard from the VMware Converter product. VMware Converter is a separate downloadable application for Windows hosts that provides an easy-to-use, scalable solution for migrations of machines, both physical to virtual and virtual to virtual. In addition to the Conversion wizard, VMware Converter provides a task manager that lets you schedule migrations of many machines.

The Conversion wizard included with Workstation lets you create VMware virtual machines from a local or remote physical machine or from virtual machines and system images that were originally created by using other products than VMware products. You can also use the wizard to change a virtual machine using one VMware format to that using another. For example, you can copy a VMware Server virtual machine and use it to create an ESX virtual machine.

To use other features of VMware Converter, such as its task manager, or the ability to import more than one virtual machine at a time, download the VMware Converter.

Supported Source Machines

The VMware Conversion wizard in Workstation allows you to import the following types of physical and virtual machines:

- Physical machines
 - Windows 2000
 - Windows 2003 32-bit and 64-bit
 - Windows XP Professional 32-bit and 64-bit

NOTE The VMware Conversion wizard included with Workstation does not convert Windows Vista physical machines to virtual machines. It also does not support converting Windows Vista images.

- VMware virtual machines (.vmx and .vmtn files)
 - Workstation 4.x, 5.x, and 6.0.x (for this beta release, Workstation 6.5 virtual machines are not yet supported)
 - VMware Fusion 1.x
 - VMware Player 1.x and 2.x
 - ESX Server 3.x
 - ESX Server 2.5.x (if the virtual machine is managed with VirtualCenter 2.x)

- GSX Server 3.x
- VMware Server 1.x
- VirtualCenter 2.x
- Virtual appliances

Appliances that use open virtual machine format (.ovf and .ova files) and that use VMware virtual hard disks (.vmdk files) or Microsoft Virtual PC or Virtual Server virtual hard disks (.vhd files)
- Other virtual machines and system images
 - Acronis True Image 9 (.tib files)
 - StorageCraft ShadowProtect (.spf files)
 - Microsoft Virtual PC 7.x and higher (.vmc files)
 - Any version of Microsoft Virtual Server (.vmc files)
 - Symantec Backup Exec System Recovery (formerly LiveState Recovery) 6.5 and 7.0, LiveState Recovery 3.0 and 6.0 (.sv2i files)
 - Norton Ghost images 9.x and higher (.sv2i files)

The operating system on the source Microsoft Virtual PC or Virtual Server virtual machine must be a Windows 2000 or later guest operating system supported by the intended VMware platform (for example, Workstation 4, 5, or 6). For a list of supported operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site.

NOTE Virtual machines from Macintosh versions of Virtual PC are not supported.

Operating System Compatibility

To import a virtual or physical machine or a third-party image, the operating system on which Workstation is installed must be equal to or greater than the operating system on the source machine. For example, if Workstation is installed on a Windows 2000 machine, you cannot import a virtual machine from a Windows XP or Windows 2003 source machine.

Importing from Various Sources

Keep these points in mind when using the Conversion wizard.

Source Type Selection

On the Source Type page of the wizard, if you are not sure which source type to choose, you can take a guess. For example, if you are not sure whether to choose **Other Virtual**

Machine or **Backup Image** for a StorageCraft ShadowProtect file, choose either one and when the wizard reads the file, it selects the correct source type.

Physical Machine Source

To import a remote machine, you are prompted to supply the computer name or IP address and the user name and password for logging in to the machine with administrative privileges. The user name must take the form <DOMAIN>\<user_name>.

NOTE Remote physical machines cannot be imported into an ESX-compatible format by the wizard.

Microsoft Virtual PC and Virtual Server Virtual Hard Disks

As of Workstation 6.5, a converted virtual machine can share the source Microsoft virtual hard disk (.vhd files). This means that the VMware virtual machine can write directly to the original .vhd files instead of VMware virtual hard disk (.vmdk) files.

If you select **Share source** the converted virtual machine consists of a VMware virtual machine configuration file (.vmx file) and the original .vhd file, which remains in its original location. VMware modifies the .vhd file, installing VMware-specific video drivers, device drivers for virtual network cards, and so on. The VMware-specific drivers replace the Microsoft drivers.



CAUTION If you plan to select **Share source** on the Virtual Machine Options page of the Conversion wizard, make a backup copy of the original Microsoft Virtual PC or Virtual Server before you use the wizard.

ShadowProtect and Backup Exec System Recovery Images

You can import ShadowProtect and Backup Exec System Recovery images, but keep the following limitations in mind:

- Dynamic disks are not supported.
- All images for the backup of a machine should be in a single folder, with no other images placed there.
- All volumes in the disk up to the active and system volumes must be backed up. For example, if a disk has four partitions, 1–4, with partition 2 as the active volume and partition 3 as the system volume, the backup must include 1 through 3.
- If it is an incremental image, up to 16 incremental backups are supported.
- For ShadowProtect, images of systems with logical drives are not supported if the logical drive is also a system or active volume.

Appliances That Use Open Virtual Machine Format

Open virtual machine format (OVF) is a platform-neutral, secure, and portable format for packaging and distributing virtual appliances. Although OVF does not rely on a specific virtualization platform, the Conversion wizard supports only OVF appliances that use VMware virtual hard disks (.vmdk files) and Microsoft Virtual PC or Virtual Server virtual hard disks (.vhd files).

In the Conversion wizard, you can select .ovf files, which are the OVF equivalent of a VMware virtual machine configuration file (.vmx file), or you can select .ova files (open virtual appliance files). An .ova file stores the configuration file and virtual hard disk file together, like a .zip file, for easy distribution.

When specifying the location of the OVF appliance, you can browse to a directory or use a URL to download the appliance from a Web server. You can also download the appliance from a secure (HTTPS) Web server.

NOTE When you use a URL, the virtual appliance is downloaded before the conversion process starts. Downloading can take 15 minutes or longer, depending on the size of the file. During the download, the progress bar in the wizard does not move.

The Conversion wizard always makes a full clone when it converts an OVF appliance to a virtual machine. See [“Full or Linked Clones”](#) on page 143.

Dual-Boot System Source

When you import a physical machine that is part of a dual-boot system, you can import only the default operating system to which `boot.ini` points. To import the nondefault operating system, change `boot.ini` to point to the other operating system and reboot before attempting to import.

Windows NT Virtual Machine Source

If the source virtual machine is Windows NT SMP, the wizard might require files from service packs or hot fixes. The wizard shows which files it requires. You must browse to the required files. They can be on a disk, your local system, or the network.

On Windows NT machines, during the import process, a snapshot driver is downloaded to the machine. This driver handles the copying and moving of files and registry settings. The driver requires a reboot to complete its tasks. When it is finished, the driver is uninstalled.

NOTE For this beta release, although Windows NT virtual machines are supported as a source, Windows NT physical machines are not supported.

ESX Virtual Machine Source

You must supply the name of the ESX server and the user name and password for logging in.

Password-Protected Virtual Machines

If the virtual machine you want to import is password protected, you must supply the password.

About Page Files and Hibernation Files

You can import all the disks for the physical or virtual machine or, to save space, you can select some of the volumes and leave out others. If you select specific volumes, you can also ignore the page and hibernation files. These files are large and, for volume-based cloning, do not provide information that you need to copy.

Supported Volume Types

Some types of source volumes, or partitions, are unsupported and are skipped during cloning. Virtual machine importing supports basic volumes and all types of dynamic volumes except RAID. Only Master Boot Record (MBR) disks are supported. GUID Partition Table (GPT) disks are not supported.

Disk Space Allocation

As is the case when you use the New Virtual Machine wizard, you must specify whether to allocate all the space at creation time or allow the files to grow. Allocating space at creation time gives better performance but is a time-consuming process. VMware recommends that you allow the disk to grow.

Select the option **Split disk into 2GB files** if your virtual disk is stored on a file system that does not support files larger than 2GB.

Full or Linked Clones

If the source is a virtual machine, you can create a full or linked clone. On the Virtual Machines Options page of the Conversion wizard, select **Import and Convert** to create a full clone. Select **Share source and store changes separately** to create a linked clone.

NOTE For Microsoft Virtual PC and Virtual Server virtual machines, you have a third option. Instead of creating a full or linked clone, you can have the converted virtual machine use the original Microsoft virtual hard disk. This option modifies the source virtual machine. See [“Microsoft Virtual PC and Virtual Server Virtual Hard Disks”](#) on page 141.

Linked clones can be created from VMware virtual machines, Symantec Backup Exec System Recovery virtual machines (.sv2i files), Microsoft Virtual PC and Virtual Server virtual machines, Acronis True Image (.tib files), and StorageCraft files (.spf files). Creating a linked clone of a VMware virtual machine requires that the virtual hardware version of the destination machine not be higher than the hardware version of the source.



CAUTION For linked clones, the virtual machine created by the wizard becomes corrupted if the source is modified after the import. This is true for linked clones imported from Virtual PC and Virtual Server machines and from Symantec backup images. In the case of Virtual PC and Virtual Server source virtual machines, powering them on in Virtual PC or Virtual Server modifies them.

Supported Destinations

The Conversion wizard can create virtual machines that are compatible with the following products:

- Workstation 4.x, 5.x, and 6.0.x (for this beta release, Workstation 6.5 virtual machines are not yet supported)
- VMware Fusion 1.x
- VMware Player 1.x and 2.x
- ESX Server 3.x (This destination is not supported if you are importing a remote physical machine.)
- ESX Server 2.5.x (This destination is supported only by importing through a VirtualCenter 2.x server that manages the 2.5.x ESX Server.)
- GSX Server 3.x
- VMware Server 1.x
- VirtualCenter 2.x

NOTE Workstation 4 virtual machines are compatible with VMware GSX Server 3.0, ESX Server 2.x, and ACE 1.x.

Designating a Destination for a Virtual Machine

Keep these points in mind when using the Conversion wizard to specify a destination for a newly created virtual machine.

ESX Virtual Machine Destination

You must supply the name of the ESX server and the user name and password for logging in.

VirtualCenter Virtual Machine Destination

You must provide the following information:

- Name of the VirtualCenter server and the user name and password for logging in.
- Name of the folder in the VirtualCenter inventory where you want to store the virtual machine.
- Name of the host, cluster, or resource pool within a host or cluster from which the virtual machine is to be run. If you select a cluster in manual mode, you must also choose a specific host.
- Name of the datastore for the virtual machine's configuration files and disks. Use the advanced setting to distribute the virtual machine's disks over multiple datastores.

Network Adapters

You are prompted to choose from the available networks at the destination location. For more information about networking choices for virtual machines used with Workstation rather than ESX or Virtual Center, see [“Common Networking Configurations”](#) on page 260.

Optional Guest Operating System Customization

You can make changes to the identity of the virtual machine (such as computer name and security ID), networking information, and so on with the wizard. For virtual machines that are converted to ESX virtual machines, you can have the wizard install VMware Tools.

You can make the following customizations:

- Computer information
 - **Computer name** – Alphanumeric name of up to 63 characters. Hyphens and underscores are allowed.
 - **Security ID (SID)** – Optionally, generate a new security ID.
 - **Sysprep file location** – If the wizard can detect the location, the wizard page displays it. Otherwise, you need to supply the location.
- Windows licensing information

- **Product ID** – Optional.
- **Windows Server license information** – For Microsoft Windows 2000 Server and 2003 Server only.
- Time zone
- Network information
 - **Network adapter (interfaces)** – Reset to default or make changes.
 - **DHCP** – Choose between using DHCP to obtain IP addresses or entering them manually. You can also use DHCP to obtain a DNS server address or enter it manually.
 - **DNS** – Enter DNS suffixes and customize their order to specify the order in which a virtual machine uses them to make connections.
 - **WINS** – Specify primary and secondary WINS addresses.
 - **Workgroup or domain** – For workgroups, specify the workgroup name, up to 15 characters. For domains, specify the Windows Server domain, along with the appropriate user name and password.

Conversion Impact on Settings

The VMware virtual machine created by the Conversion wizard contains an exact copy of the disk state from your source virtual machine or system image, with the exception of some hardware-dependent drivers and, sometimes, the mapped drive letters.

The following settings from the source computer remain identical:

- Operating system configuration (computer name, security ID, user accounts, profiles and preferences, and so forth)
- Applications and data files
- Each disk partition's volume serial number

Because the target and the source virtual machines or system images have the same identities (name, SID, and so on), running both on the same network can result in conflicts. If you plan to redeploy the source virtual machine or system image, do not run both the source and target images or virtual machines on the same network at the same time.

Alternatively, you can resolve the duplicate ID problem by using additional tools, such as the Windows 2000 System Preparation Tool (Sysprep). For example, if you use the Conversion to test the viability of running a Virtual PC virtual machine as a VMware

virtual machine without first decommissioning the original Virtual PC machine, you need to resolve the duplicate ID problem.

Migration Issues Caused by Hardware Changes

Most migrated applications function correctly in the VMware virtual machine because their configuration and data files have the same location as the source virtual machine. However, applications might not work if they depend on specific characteristics of the underlying hardware such as the serial number or the device manufacturer.

When troubleshooting after virtual machine migration, consider the following potential hardware changes:

- The CPU model and serial numbers (if activated) can be different after the migration. They correspond to the physical computer hosting the VMware virtual machine.
- The Ethernet adapter can be different (AMD PCNet or VMXnet) with a different MAC address. Each interface's IP address must be individually reconfigured.
- The graphics card can be different (VMware SVGA card).
- The numbers of disks and partitions are the same, but each disk device can have a different model and different manufacturer strings.
- The primary disk controllers can be different from the source machine's controllers.
- Applications might not work if they depend on devices that are not available from within a virtual machine.

Open a Third-Party Virtual Machine or System Image

The **File > Open** command lets you convert a system image or virtual machine created with software from another company into a VMware virtual machine.

To convert a virtual machine or system image using the Open command

- 1 From the Workstation menu bar, choose **File > Open**.
- 2 In the **File name** field, browse to and open the configuration (.vmx, .vmc, .spfv, or .sv2i) file for the virtual machine or system image to convert.

You can use the field **Files of type** to filter the files displayed by file extension.

- 3 Click **Open**.

Workstation creates a VMware virtual machine, with a VMware configuration file (.vmx) for the converted virtual machine or system image. The converted virtual machine links to the virtual disks of the original virtual machine or system image. The original Virtual PC, Symantec Backup Exec System Recovery, or StorageCraft configuration (.vmc, .spf, or .sv2i) file is unchanged.

If you attempt to open a virtual machine or system image that is password protected, you are prompted to use the Conversion wizard. See [“Import a Virtual Machine, Virtual Appliance, or System Image”](#) on page 148.

Import a Virtual Machine, Virtual Appliance, or System Image

The **File > Import** command enables you to convert a system image or virtual machine into a VMware virtual machine.

Before you begin, review the restrictions and requirements for source and destination virtual machines. See [“Supported Source Machines”](#) on page 139 and [“Supported Destinations”](#) on page 144.

To import a virtual machine, virtual appliance, or system image

- 1 If you are importing a virtual machine, make sure the virtual machine is powered off.
- 2 Choose **File > Import** to launch the VMware Conversion wizard.
- 3 Complete the wizard pages.

The text on the wizard pages changes, depending on the selections you make. For example, on the Source Type page, when you select a source type from the drop-down list, the text below the list changes to describe which types of virtual machines are included in that source type.

As you proceed through the wizard, the navigation pane on the left side of the wizard helps track your progress.

Whenever you start a new phase or step, a list expands to display the names of the wizard pages included in that step. When you complete an entire step, the next step expands.

To go back to a previous page, click its name in the navigation pane.

Getting Started with Virtual Machines

8

This chapter includes the following topics:

- [“Starting a Virtual Machine”](#) on page 149
- [“Shut Down a Virtual Machine”](#) on page 152
- [“Delete a Virtual Machine”](#) on page 153
- [“Controlling the Display”](#) on page 154
- [“Install New Software in a Virtual Machine”](#) on page 165
- [“Use Removable Devices in a Virtual Machine”](#) on page 166
- [“Using VNC for Remote Connections to a Virtual Machine”](#) on page 167
- [“Set Up Appliance View for a Virtual Machine”](#) on page 169
- [“Create a Screenshot of a Virtual Machine”](#) on page 171
- [“Create and Play Back a Movie of a Virtual Machine”](#) on page 171
- [“Advanced Options for Application Developers”](#) on page 173

Starting a Virtual Machine

Starting a virtual machine means displaying its running console so that you can interact with it. Depending on the situation, starting a virtual machine can involve any of the following:

- To start a virtual machine from the Workstation user interface, you must open the virtual machine and power it on.
- To start a virtual machine that is running in the background when Workstation is not running, you must open its console from the taskbar on the host.

- To start a virtual machine that is available from a Web server, you must use a command-line command to begin streaming the virtual machine and then start it from the Workstation window.
- To start a virtual machine from the command line, you must use the platform-specific program and startup options. See [“Startup Options for Workstation and Virtual Machines”](#) on page 455.

Start a Virtual Machine from the Workstation User Interface

Before you begin, make sure that all of the virtual machine files are accessible to the host where Workstation is installed.

To start a virtual machine from the Workstation user interface

- 1 Start Workstation.
For instructions, see [“Start Workstation on a Windows Host”](#) on page 61.
- 2 Choose **File > Open** and browse to the configuration (.vmx) file for the virtual machine you want to use.
See [“Virtual Machine Location”](#) on page 151.
- 3 Click the **Power On** button to start the virtual machine.
- 4 Click anywhere inside the virtual machine console to give the virtual machine control of your mouse and keyboard.
- 5 If you need to log on to the operating system in the virtual machine, type your name and password just as you would on a physical computer.

You can add the name of the virtual machine to the **Favorites** list so that you do not need to browse to the file to open the virtual machine. See [“Favorites List in the Sidebar”](#) on page 72.

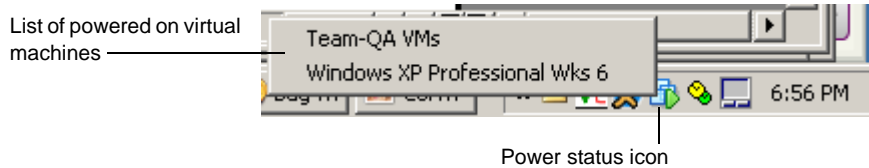
Start a Virtual Machine That Is Running in the Background

If you do not power off a virtual machine when you exit Workstation, the virtual machine continues running in the background. To start the virtual machine, use the power status icon on the host to open the virtual machine's console.

By default Workstation is configured to display a power status icon in the notification area of the host's taskbar even when Workstation is not running. If this icon is not visible, before you begin, use the **Workspace** tab of the Workstation preferences editor to display it. See [“Introduction to Workstation Preferences”](#) on page 76.

To start a virtual machine that is running in the background

- 1 Click the power status icon in the notification area of the host's taskbar.
- 2 Click the tooltip that appears to display a list of the virtual machines.



This list contains the virtual machines and teams that belong to the logged in user.

- 3 Click the machine you want to open.

Workstation starts and displays the console view of the virtual machine.

Virtual Machine Location

By default, virtual machine files are stored in the virtual machine's working directory:

- On Windows hosts, Workstation stores virtual machines in the My Documents folder of the user who is logged on at the time the virtual machine is created.

On Windows Server 2003, Windows XP and Windows 2000, the default folder is:

C:\Documents and Settings\<username>\My Documents\My Virtual Machines\<guestOSname>

On Windows Vista, the default folder is:

C:\Users\<username>\Virtual Machines\<guestOSname>

- On Linux hosts, Workstation stores virtual machines in:

<homedir>/vmware/<guestOSname>

Here <homedir> is the home directory of the user who is logged on at the time the virtual machine is created.

The working directory is also where Workstation stores suspended state (.vmss), snapshot (.vmsn), and redo log files. The **General** tab of the virtual machine settings editor displays the path to the working directory. See [“Introduction to Virtual Machine Settings”](#) on page 79.

Shut Down a Virtual Machine

As with physical computers, you can shut down a guest operating system before you power off the virtual machine or team.

You are not required to shut down the guest before exiting Workstation. If you want to exit Workstation but leave the virtual machine running in the background, see [“Closing Virtual Machines and Exiting Workstation”](#) on page 81.

To shut down a virtual machine

- 1 In the guest system, shut down the operating system as you would if you were using a physical machine rather than a virtual machine.

For example, in Windows XP, click **Start > Shut Down**.

- 2 In the Workstation menu bar, choose **VM > Power Options > Power Off** to turn off the virtual machine.

If you use the **Power Off** command before you shut down the guest operating system, the virtual machine is powered off abruptly. The effect is like using the power button on a physical machine. You can, however, configure the **Power Off** button in the toolbar to shut down the operating system before powering off. See [“Configure Power Off and Reset Options for a Virtual Machine”](#) on page 152.

Configure Power Off and Reset Options for a Virtual Machine

You can configure the **Power Off** toolbar button to power off the virtual machine abruptly or to send a signal that gracefully shuts down the guest operating system.

Before you begin, make sure VMware Tools is installed in the guest operating system. To perform a graceful shutdown, the VMware Tools service component issues a **Shutdown Guest** command and runs a script to shut down cleanly.



CAUTION Powering off abruptly works the same way a power switch works on a power supply. The power is cut off with no consideration for work in progress. If a virtual machine is writing to disk when it receives a **Power Off** command, data corruption might occur.

Similarly, you can configure the **Reset** button to work the same way as a reset switch, so that it resets the virtual machine abruptly. Or you can set the **Reset** button so that the VMware Tools service sends a restart signal to the guest operating system. It then shuts down gracefully and restarts.

Not all guest operating systems respond to a shutdown signal from the **Power Off** button, or to a restart signal from the **Reset** button. If your operating system does not

respond to the signal, shut down or restart from the operating system, as you would with a physical machine.

To configure the Power Off and Reset options for a virtual machine

- 1 Select the virtual machine.
The virtual machine can be powered on or off.
- 2 Choose **VM > Settings**.
- 3 Click the **Options** tab and select **Power**.
- 4 In the **Power Controls** section of the dialog box, specify whether you want the **Power Off** button to shut down the guest gracefully or to abruptly power the virtual machine off.

The selection you make is reflected in the tooltip you see when you place your mouse pointer over the **Power Off** toolbar button.

- 5 Specify how you want the **Reset** button to work.
- 6 If you want to change any of the other settings and need more information, click **Help**.

For UNIX guests, if you want to pass X toolkit options when you power on a virtual machine, see [Appendix A, “Workstation Command-Line Reference,”](#) on page 455.

Delete a Virtual Machine

You can use a Workstation command to delete a virtual machine and all its files from the host file system.

If, instead of deleting the virtual machine altogether, you want to remove it from the **Favorites** list or from a team, see [“Remove an Item from the Favorites List”](#) on page 74 and [“Remove a Virtual Machine from a Team”](#) on page 251. Open the team, as described in [“Open a Team and Add It to the Favorites List”](#) on page 247. In the summary view for the team, in the **Virtual Machines and LAN Segments** section, right-click the name of the virtual machine, and choose **Remove from Team**.



CAUTION Do not delete a virtual machine if it was used to make a linked clone virtual machine and you still want to use the linked clone. If the linked clone cannot find the virtual disk files from the parent virtual machine, the linked clone will no longer work.

To delete a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Delete from Disk**.

Controlling the Display

You can control the Workstation display to suit the way you prefer to work with virtual machines. For example, you can use full screen mode to hide the host user interface altogether, or you can use unity mode so that applications from the virtual machine appear on the host desktop and hide the rest of the virtual machine user interface.

Using Unity Mode

In virtual machines with some guest operating systems, you can switch to unity mode to display applications directly on the host desktop. The virtual machine console view is hidden, and you can minimize the Workstation window.

Your taskbar displays items for open applications in unity mode just as it does for open host applications.

NOTE If you save a file or attempt to open a file from within an application in unity mode, the file system you see is the file system inside the virtual machine. You cannot open a file from the host operating system or save a file to the host operating system.

When a virtual machine is in unity mode, you can access the virtual machine's **Start** menu (for Windows virtual machines) or **Applications** menu (for Linux virtual machines) by placing the mouse pointer over the host's **Start** or **Applications** menu.

For this beta release, the unity feature has the following limitations:

- Only newer versions of Windows guests are supported. These include Windows 2000 and higher. Linux guests can sometimes use unity mode.
- You can copy and paste text but not files between the host and guests in unity mode. Neither can you drag and drop files between host and guest.
- If you have multiple monitors, application windows in unity mode can appear only on the monitor that is set as the primary display. On Windows hosts, this setting is configured in your Control Panel's Display Settings.
- Applications run more slowly than they would be in console view or full screen mode.

Set Preferences for Unity Mode

NOTE For this beta release, setting preferences for unity mode is available on Linux hosts only.

You can configure access to a virtual machine's **Start** or **Applications** menu from a Windows **Start** menu or Linux **Applications** menu on your host's desktop. You can also specify which color to make the border around applications that run in unity mode on your desktop.

To help distinguish between the application windows that belong to various virtual machines, you can give them different colors. For example, you can set the applications for one virtual machine to have a blue border and set the applications for another virtual machine to have a yellow border.

To set preferences for unity mode

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 Click the **Options** tab and select **Unity**.
- 5 Complete the settings panel and click **OK**.

Use the following information to determine which features to enable:

- If you specify that you want to use a custom color, click the colored rectangle to access the color chooser.
- If you enable a **Start** menu for a Windows virtual machine or **Applications** menu for a Linux virtual machine the menu appears above the host's **Start** or **Applications** menu.

Use this feature for easy access to applications in the virtual machine that are not open in unity mode. If you do not enable this feature, you must exit unity mode to display the virtual machine's **Start** or **Applications** menu in the console view.

Go into and out of Unity Mode

In unity mode, a virtual machine's applications look just like other application windows on the host, except that they have a colored window border and a VMware logo in the window's title bar.

Before you begin, make sure the virtual machine meets these requirements:

- The virtual machine must be a Workstation 6 or higher virtual machine.
- VMware Tools must be installed and running in the virtual machine's guest operating system. The version of VMware Tools must be the version included in Workstation 6.5 or higher. For instructions, see [“Installing VMware Tools”](#) on page 105.
- The guest operating system in the virtual machine must be Windows 2000 or higher. Linux guests can sometimes use unity mode.
- For Linux guests and hosts, VMware recommends that you use one of the newer window managers, such as Metacity or Compiz.

To go into and out of unity mode

- 1 In the virtual machine, open the applications you want to use in unity mode.
- 2 From the Workstation menu bar, choose **View > Unity**.

A check mark appears next to **Unity** in the menu.

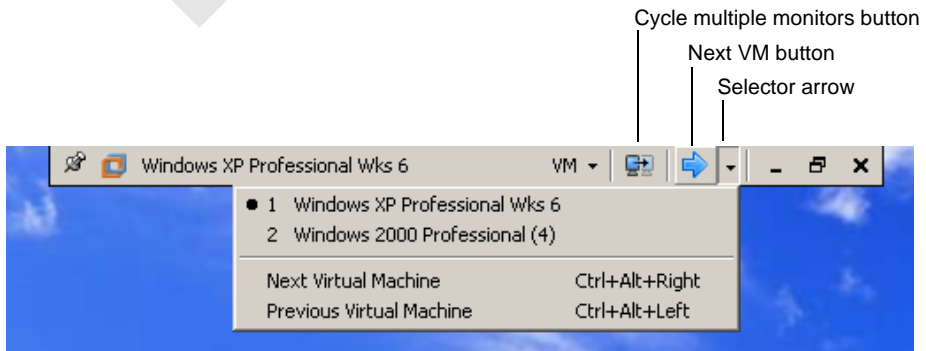
The virtual machine's console view in the Workstation window is hidden, and the guest's open applications are displayed in application windows on the host's desktop.

- 3 To exit unity mode, display the Workstation window and choose **View > Unity** to remove the check mark next to **Unity**.

Use Full Screen Mode

In full screen mode, the virtual machine display fills the screen, so that you no longer see the borders of the Workstation window.

Figure 8-1. Full Screen Toolbar on a Windows Host



Before you begin, make sure the guest operating system has VMware Tools installed. See [“Installing VMware Tools”](#) on page 105.

NOTE If you plan to run the virtual machine in full screen mode on a laptop computer, also see [“Report Battery Information in the Guest Operating System”](#) on page 158.

To use full screen mode

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered on.
- 3 If you have multiple monitors, move the Workstation window into the monitor you want to use for displaying the virtual machine in full screen mode.
- 4 Choose **View > Full Screen**.

If you cannot enter full screen mode when the guest’s display mode is smaller than the host’s display mode, try adding the following line to the virtual machine’s configuration (.vmx) file:

`mks.maxRefreshRate=1000`

For more information about the configuration file, see [“Files That Make Up a Virtual Machine”](#) on page 100.
- 5 (Optional) To switch from full screen mode back to windowed mode, which shows your virtual machine inside a Workstation window again, press Ctrl+Alt+Enter.
- 6 (Optional) To hide the full screen toolbar and menus while you are using full screen mode, click the push pin icon and move your mouse pointer off of the toolbar.

This action unpins the toolbar. The toolbar slides up to the top of the monitor and disappears. To display the toolbar again, move the mouse pointer to the top of the screen until the toolbar appears.
- 7 (Optional) To switch from one powered-on virtual machine to another while in full screen mode, do one of the following:
 - To go to a specific powered-on virtual machine, click the virtual machine arrow, as shown in [Figure 8-1](#), and select the virtual machine.
 - To go to the next virtual machine, press Ctrl+Alt+right arrow, or press Ctrl+Alt+left arrow to go to the previous virtual machine.
- 8 (Optional) Use the **VM** menu on the toolbar to access any of the commands that you normally see in the Workstation **VM** menu.

To display the virtual machine across two or more monitors in full screen mode, see [“Use Multiple Monitors for One Virtual Machine”](#) on page 160.

Report Battery Information in the Guest Operating System

If you run a virtual machine on a laptop in full screen mode, configure the option to report battery information in the guest. This way, you can determine when the battery is running low.

To report the status of the battery in the guest

- 1 Start Workstation and select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 Click the **Options** tab and select **Power**.
- 5 Select the **Report battery information to guest** check box and click **OK**.

Use Quick Switch Mode

In quick switch mode, the virtual machine's screen is resized to fill the screen completely, except for the space occupied by the tabs.

Before you begin, make sure the guest operating system has VMware Tools installed. See [“Installing VMware Tools”](#) on page 105.

Quick switch mode is similar to full screen mode with the addition of tabs at the top of the screen for switching from one virtual machine to another. The other difference is that you can use quick switch mode with virtual machines that are powered on or off.

To use quick switch mode

- 1 Select the virtual machine.
- 2 Choose **View > Quick Switch**.
- 3 (Optional) To view the Workstation menu and toolbar while using quick switch mode, move the mouse pointer to the top of the screen.
- 4 (Optional) To resize a guest operating system's display so it fills as much of the screen as possible in quick switch mode, choose **View > Fit Guest Now**.
- 5 To get out of quick switch mode, move the mouse pointer to the top of the screen to activate the menu and choose **View > Quick Switch**.

Use Exclusive Mode

You might want to use exclusive mode to run graphics-intensive applications, such as games, in full screen mode.

Before you begin, make sure the guest operating system has VMware Tools installed. See [“Installing VMware Tools”](#) on page 105.

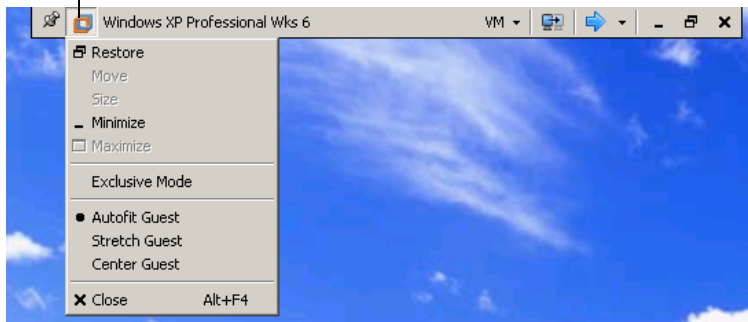
Like full screen mode, exclusive mode causes the Workstation virtual machine display to fill the screen. Drawbacks to using exclusive mode include the following:

- The full screen toolbar is not available in exclusive mode. To configure any virtual machine settings, you need to leave exclusive mode (by pressing Ctrl+Alt).
- Exclusive mode does not use more than one monitor.
- Exclusive mode causes the host resolution to resize, which can cause items on the host desktop to be moved.

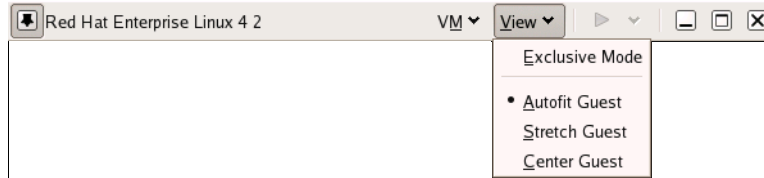
To use exclusive mode

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered on.
- 3 If you have multiple monitors, move the Workstation window onto the monitor you want to use.
- 4 Press Ctrl+Alt+Enter to enter full screen mode.
- 5 On the full screen toolbar, do one of the following:
 - On Windows hosts, click the **Workstation** icon to display the system menu and choose **Exclusive Mode**.

System menu



- On Linux hosts, click the **View** menu on the full screen toolbar and choose **Exclusive Mode**.



- 6 To exit full screen mode and return to windowed mode, press Ctrl+Alt.

Use Multiple Monitors for One Virtual Machine

If your host has a multiple-monitor display, you can configure a virtual machine to use two or more monitors.

On Windows guests, you do not need to use the Windows display properties settings to configure multiple monitors.

Before you begin, make sure the virtual machine meets these requirements:

- The virtual machine is a Workstation 6 or higher virtual machine.
- VMware Tools is installed and running in the virtual machine's guest operating system. The version of VMware Tools must be the version included in Workstation 6 or higher. For instructions, see ["Installing VMware Tools"](#) on page 105.
- The guest operating system in the virtual machine is Windows XP, Windows Vista, or Linux.
- On the host, the display settings for monitors must be set in a compatible topology. For example, the left-most monitor cannot be below any other monitor. It does not matter if the monitors have different resolutions or orientations. When entering full screen mode, the monitor containing the Workstation window cannot be below another monitor.

Put another way: When you use the Windows display properties controls, if you select a monitor icon and begin to drag it to a new location, a pop-up displays the coordinates. If a coordinate shown for the new location of the icon is a negative number, that location will not work.

To use multiple monitors for one virtual machine

- 1 Choose **Edit > Preferences**.
- 2 Click the **Display** tab and in the **Full Screen** section, select **Autofit guest** and click **OK**.
- 3 Select a virtual machine.
- 4 Make sure the virtual machine is powered off.
- 5 Choose **VM > Settings**.
- 6 On the **Hardware** tab, select **Display**.

If **Display** does not appear in the list on the **Hardware** tab, it probably means that the virtual machine is a Workstation 4 or 5 virtual machine. Only Workstation 6 or higher virtual machines have this feature.

- 7 On the settings panel for the **Display** tab, specify how to determine the number of monitors.

In most cases, select **Use host setting for monitors**. This option means that if the virtual machine is run on a host that is using one monitor, the virtual machine will see only one monitor. But if the same virtual machine is moved to a host that is using two monitors, the virtual machine will see two monitors.

Here, the number of monitors depends on the number of monitors the host recognizes when it starts up. For example, if you power on a laptop that is undocked, the host setting is one monitor, even if you later place the running laptop in a docking station that uses two monitors.

Similarly, if the host has one monitor and you suspend the virtual machine and change the host to have two monitors, when you resume the virtual machine, it is still configured to use one monitor. You must restart the virtual machine to detect the new settings.

You might want to set a specific number of monitors if, for example, you are writing an application to be displayed on multiple monitors but the host you are using has only one monitor.

- 8 If you set a specific number of monitors, also specify a sufficient maximum resolution.

The resolution of a host monitor that you use to display the virtual machine must not exceed the **Maximum resolution** setting you specify here.

- 9 Power on the virtual machine and choose **View > Full Screen**.

For more information, see [“Use Full Screen Mode”](#) on page 156.

Make sure the virtual machine is completely powered on. If when you power on the virtual machine, it is set to be restored from a snapshot and if background snapshots are enabled, powering on might take longer. In this case, displaying the virtual machine to two monitors might not work correctly at first. If you see this issue, go to **Edit > Preferences > Priority** deselect the check box called **Take and restore snapshots in the background**.

- 10 On the full screen toolbar, click the **Cycle Multiple Monitors** button.

This button is available only if the host has more than one monitor. This button is shown in [Figure 8-1, “Full Screen Toolbar on a Windows Host,”](#) on page 156.

Clicking the **Cycle Multiple Monitors** button causes the guest operating system's desktop to extend to the additional monitor or monitors.

If the virtual machine does not display correctly, use the system menu (on Windows hosts) or the **View** menu (on Linux hosts) and make sure **Autofit Guest** is selected.

- 11 If you have more than two monitors, and you want the virtual machine to use them, click the **Cycle Multiple Monitors** button again.

The ordering in which the monitors are used depends on the order in which the monitors were added to the host operating system.

- 12 To return to using only one monitor, click the **Cycle Multiple Monitors** button until the display returns to one monitor.

Use Multiple Monitors for Multiple Virtual Machines

If your host has a multiple-monitor display, you can run a different virtual machine on each monitor.

Before you begin, make sure the guest operating system has VMware Tools installed. See [“Installing VMware Tools”](#) on page 105.

To use multiple monitors for multiple virtual machines

- 1 To open multiple Workstation windows, choose **File > New > Window**.

On Linux hosts, although you can have multiple Workstation windows, the windows operate in a single Workstation process, which saves memory and allows preferences and **Favorites** list items to be shared.

- 2 (Optional) On Linux hosts, if you want to run separate Workstation processes in different X servers, start the second instance of Workstation with the **-W** flag.

In a terminal window, enter the following command:

```
vmware -W &
```

- 3 Start one or more virtual machines in each Workstation window.

If you have a virtual machine running in one window and you want to run that virtual machine in another Workstation window, be sure to close the virtual machine in the first window before attempting to open it in another.

- 4 Drag each Workstation window to the monitor on which you want to use it.
- 5 To switch mouse and keyboard input from the virtual machine on the first screen to the virtual machine on the second screen, move the mouse pointer from one to the other and click inside the second screen.

If you changed the defaults, you might need to press Ctrl+Alt to release the mouse pointer from the first virtual machine.

Fitting the Workstation Console to the Virtual Machine Display

The **Autofit** and **Fit** commands in the **View** menu allow you to match the Workstation console with the guest operating system display size.

With both **Autofit** commands toggled off, Workstation does not automatically match window sizes as you work. Scroll bars appear in the console when the Workstation console is smaller than the guest operating system display. A black border appears in the console when the console is larger than the guest operating system display.

The **Autofit** and **Fit** commands are described [Table 8-1](#).

Table 8-1. Autofit and Fit Commands

View Menu Command	Description
Autofit Window	Causes the Workstation console to maintain the size of the virtual machine's display resolution. If the guest operating system changes its resolution, the Workstation console resizes to match the new resolution.
Autofit Guest	Causes the virtual machine to resize the guest display resolution to match the size of the Workstation console.
Fit Window Now	Causes the Workstation console to match the current display size of the guest operating system.
Fit Guest Now	Causes the guest operating system display size to match the current Workstation console.

An **Autofit** command is toggled on or off each time you select it. If **Autofit Window** and **Autofit Guest** are toggled on, you can manually resize the Workstation console, but the guest operating system can also resize the Workstation console.

The **Fit Window Now** or **Fit Guest Now** command is redundant if the corresponding Autofit command is active because the console and the guest operating system display are the same size.

Considerations for Display Resizing in Linux Guests

For Linux guests, the following considerations apply to display resizing:

- If you have virtual machines that were suspended under a version of VMware Tools before version 5.5, display resizing will not work until the virtual machines are completely powered off and powered on again. (Rebooting the guest operating system is not sufficient.)
- Update VMware Tools to the latest version in the guest for the display resizing options to work.
- Before you can use the **Autofit Guest** and **Fit Guest Now** options, VMware Tools must be running.
- All the restrictions on resizing that the X11 Windows system imposes on physical hosts apply to guests.
 - You cannot resize to a mode that is not defined. The VMware Tools configuration script can add a large number of mode lines, but you cannot get 1-pixel granularity as in Windows. VMware Tools adds modelines in 100-pixel increments. This means you cannot resize a guest larger than the largest mode defined in your X11 configuration file. If you attempt to resize larger, a black border appears and the guest stops growing.
 - The X server always starts up in the largest resolution that is defined. This cannot be avoided. The XDM/KDM/GDM login screen always appears at the largest size. But both Gnome and KDE allow you to specify your preferred resolution, so you can reduce the guest display size after you log in.

Considerations for Display Resizing in Solaris Guests

For Solaris 10 guests, the following considerations apply to display resizing:

- Update VMware Tools to version 6.0 or higher in the guest for the display resizing options to work.
- Before you can use the **Autofit Guest** and **Fit Guest Now** options, VMware Tools must be running.
- Solaris 10 guests must be running an Xorg X server and JDS/Gnome.

Working with Nonstandard Resolutions

A guest operating system, and its applications, might react unexpectedly when the Workstation console size is not a standard VESA resolution (640×480, 800×600, 1024×768, and so on).

For example, the **Autofit Guest** and **Fit Guest Now** commands allow your guest operating system screen resolution to be set smaller than 640×480, but some installers do not run at resolutions smaller than 640×480. Programs might refuse to run. Error messages might include such phrases as “VGA Required to Install” or “You must have VGA to install.”

Use one of the following strategies to work around this problem with nonstandard resolutions:

- If your host computer’s screen resolution is high enough, you can enlarge the window and choose **Fit Guest Now**.
- If your host computer’s screen resolution does not allow you to enlarge the Workstation console sufficiently, you can manually set the guest operating system’s screen resolution to 640×480 or larger.

Install New Software in a Virtual Machine

Installing new software in a virtual machine is like installing it on a physical computer. Only a couple of additional steps are required.

To install new software in a virtual machine

- 1 Select the virtual machine.
- 2 Choose **VM > Removable Devices** and verify that the virtual machine has access to the CD-ROM drive, ISO image file, or floppy drive where the installation software is located.

For more information, see [“Add DVD or CD Drives to a Virtual Machine”](#) on page 227.

- 3 Choose **VM > Settings** and use the **Memory** settings panel on the **Hardware** tab to set the final memory size for the virtual machine.

Some applications use a product activation feature that creates a key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine might require you to reactivate the software. To minimize the number of significant changes, set the memory size.

- 4 Install VMware Tools in the guest operating system.

See [“Installing VMware Tools”](#) on page 105. Installing VMware Tools before installing the new application also minimizes the likelihood of requiring you to reactivate the software.

- 5 Install the new application according to the manufacturer's instructions.

Disable Acceleration If a Program Does Not Run

Occasionally, when you install or run software inside a virtual machine, Workstation appears to hang. In many cases, you can get past the problem by temporarily disabling acceleration in the virtual machine.

If this problem occurs, it usually occurs early in the program's execution.

To disable acceleration

- 1 Select the virtual machine.

The virtual machine can be powered off or on.

- 2 Choose **VM > Settings**.

- 3 Click the **Options** tab and select **Advanced**.

- 4 In the **Settings** section, select **Disable acceleration** and click **OK**.

This setting slows down virtual machine performance. It is recommended only for getting past the problem with running the program.

- 5 After you pass the point where the program encountered problems, repeat [Step 2](#) through [Step 4](#) and remove the check beside **Disable acceleration**.

Use Removable Devices in a Virtual Machine

You can configure a number of removable devices for use in a virtual machine, including floppy drives, DVD/CD-ROM drives, USB devices, smart card readers, and network adapters.

Some devices cannot be used by the host and guest or by multiple guests at the same time. For example, if a floppy drive is being used by the host, you must connect it to the virtual machine before you can use it in the virtual machine. To use it on the host again, you must disconnect it from the virtual machine.

For information about how to add or configure specific devices, see [Chapter 18, “Connecting Devices,”](#) on page 313 and [Chapter 12, “Using Disks and Disk Drives,”](#) on page 213.

To use removable devices in a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered on.
- 3 Choose **VM > Removable Devices > <Device_Name>** and then **Connect** or **Disconnect**.

If you choose **Edit**, a dialog box appears. Make the desired changes and click **OK**. If you need assistance, click the **Help** button to display online help.

- 4 (Optional) To connect or disconnect the device from the virtual machine, click or right-click the device icon in the notification area of the taskbar and choose **Connect** or **Disconnect**.

Using the device icon in the virtual machine taskbar is especially useful if you run the virtual machine in full screen mode.

Using VNC for Remote Connections to a Virtual Machine

VNC (Virtual Network Computing) software makes it possible to view and interact with one computer from any other computer or mobile device anywhere on the Internet.

VNC software is cross-platform, allowing remote control between different types of computers. For example, you can use VNC to view a Linux machine on your Windows PC. Open-source versions of VNC are freely and publicly available.

You can use Workstation to set a virtual machine to act as a VNC server, and users on other computers can install a VNC client (also called a VNC viewer) to connect to the virtual machine. After you set up a virtual machine as a VNC server, you can see a list of users who are remotely connected to the virtual machine and find out how long they have been connected.

Workstation does not need to be running when VNC connections are made. Only the virtual machine needs to be running, and it can be running in the background.

Configure a Virtual Machine as a VNC Server

You do not need to install any specialized VNC software in a virtual machine to set it up as a VNC server.

Before you begin, make sure the guest operating system has VMware Tools installed. See [“Installing VMware Tools”](#) on page 105.

To configure a virtual machine as a VNC server

- 1 Select the virtual machine.
The virtual machine can be powered on or off.
- 2 Choose **VM > Settings**.
- 3 Click the **Options** tab and select **Remote Display**.
- 4 Click **Enable remote display**.

After remote display is enabled and users connect to the virtual machine with a VNC client, you can use the **View Connected Users** button on this tab to see a list of the connected users.

- 5 (Optional) Specify a port number.

If you want to connect to more than one virtual machine on the same host with a VNC client, specify a unique port number for each virtual machine. VMware suggests you use a port number in the range from 5901 to 6001.

Keep in mind that certain port numbers are used by other applications, and some port numbers are privileged (meaning only the root or Administrator user can listen). For example, the VMware Management Interface uses ports 8333 and 8222. On Linux, only root can listen to ports up to port number 1024.

- 6 (Optional) Set a password for connecting to the virtual machine from a VNC client.
The password can be up to 8 characters long. Because it is not encrypted when it is sent by the VNC client, do not use a password that you use for other systems.
- 7 Click **OK**.

After you set up a virtual machine as a VNC server, you can see a list of users who are remotely connected to the virtual machine and find out how long they have been connected. Right-click the VNC icon in the status bar for the virtual machine.

Use a VNC Client to Connect to a Virtual Machine

You can install a VNC client on your host and connect to a running virtual machine.

Before you begin, determine the machine name or IP address of the virtual machine and, if applicable the VNC port number and password. See [“Configure a Virtual Machine as a VNC Server”](#) on page 167.

For information about mapping the keyboard to various languages, see [“Specify a Language Keyboard Map for VNC Clients”](#) on page 325.

The following issues are known to occur when you connect to virtual machines with a VNC client:

- You cannot take or revert to snapshots.
- You cannot change the power state of the virtual machine. That is, you cannot power on, power off, suspend, or resume. You can shut down the guest operating system, however, which might power off the virtual machine.
- You cannot copy and paste text between the host and guest operating system.
- You cannot configure the virtual machine with the virtual machine settings editor, and neither can you upgrade VMware Tools.
- Remote display does not work well if you are also using the 3-D feature. This feature is described in [“Support for Direct3D Graphics”](#) on page 308.

To use a VNC client to connect to a virtual machine

- 1 On a local or remote computer, start a VNC client.
You can use any VNC client, but not a Java viewer in a browser. If you need to download and install a VNC client, one of the many Web sites where you can buy or get one for free is the RealVNC Web site.
- 2 Make sure the client is set for hextile encoding.
For example, if you use RealVNC Viewer, under the **Preferred Encoding** option, select **Hextile**.
- 3 Make sure the client is set to use all colors.
For example, if you use RealVNC Viewer, under the **Colour Level** option, select **Full (all available colours)**.
- 4 When prompted for the VNC server name, enter the name or IP address of the host computer and the port number.
Use the format:
`<machine_name>:<port_number>`
- 5 If a password is required, enter one when prompted.

Set Up Appliance View for a Virtual Machine

If you want a virtual machine to function as an appliance, such as a Web server with a browser-based interface, set the virtual machine to display its appliance view when starting up, rather than the operating system console.

Before you begin, verify that the virtual machine is a Workstation 6 or higher virtual machine. For instructions on upgrading, see [“Change the Version of the Virtual Machine”](#) on page 57.

The appliance view displays a brief description of the type of server or appliance and provides a link that opens the browser on the host system and connects to the appliance's management console.

NOTE The appliance view cannot be displayed for virtual machines that are part of a team, just as the summary view is not displayed for individual members of a team.

To set up appliance view for a virtual machine

- 6 Select the virtual machine.
The virtual machine can be powered on or off.
- 7 Choose **VM > Settings**.
- 8 Click the **Options** tab and select **Appliance View**.
- 9 Select the **Enable appliance view** check box.
- 10 Complete the fields on this panel to create the text and images that users see when the virtual machine starts up.

Use the following information to configure the settings on this panel:

- Only the **Name** field is required.
 - Specify the TCP/IP port number that the appliance will use to serve HTTP content.
 - If you include an image file, it must be a PNG or BMP file. The maximum size is 256 x 256 pixels.
 - If you do not select **Switch to appliance view at power on**, the console view is displayed. Often this view shows only a simple display of the virtual machine's IP address and tells the user to open a browser.
- 11 Click **OK**.

When a user starts this virtual machine, the newly created appliance view is displayed. It first displays a “powering on” message and then provides a link to click in order to access the appliance's management console.

Create a Screenshot of a Virtual Machine

You can capture a screenshot of a virtual machine and save it to the clipboard, to a file, or both. On Linux hosts, saving to the clipboard works only on systems running Gnome 2.12 or higher.

By default, the image is saved as a portable network graphics (.png) file. On Windows hosts, you can also save it as a .bmp file.

To create a screenshot of a virtual machine

- 1 Specify your preferences for taking screenshots:
 - a From the Workstation menu bar, choose **Edit Preferences**.
 - b In the preferences editor, on the **Workspace** tab, use the **Save screenshots to** check boxes to specify whether you want to save the screenshot to the clipboard, a file, or both.
 - c If you select **File**, specify whether you want to save the file to your desktop or be prompted for the location when you take the screenshot.

If you select **Save to desktop**, the filename is generated automatically.

On Windows hosts, if you select **Ask for location**, when you are prompted for the filename and path, you can also change the file format to bitmap.

- d Click **OK**.
- 2 To take the screenshot, do one of the following:
 - From the Workstation menu bar, choose **VM > Capture Screen**.
 - Use the keyboard shortcut Ctrl+Alt+PrtScr (on Windows hosts) or Shift+Ctrl+PrtScr (on Linux hosts).

The keyboard shortcut works regardless of whether mouse and keyboard input is currently grabbed by the virtual machine or the host.

The Windows keyboard shortcut Ctrl+Alt+PrtScr assumes that your virtual machine is configured to ungrab keyboard and mouse input if you press Ctrl+Alt. If you configured a different shortcut for ungrabbing input, use that shortcut in combination with the PrtScr key.

Create and Play Back a Movie of a Virtual Machine

You can capture a movie of your screen activity within a virtual machine.

Before you begin, make sure you have the VMware movie decoder. Although you can capture a movie on Linux, you need to play it back on a Windows machine. The VMware CODEC (coder-decoder) is automatically installed with Workstation on Windows hosts. A separately downloadable installer is also available for playback of movies on Windows machines without Workstation. Go to the Downloads page on the VMware Web site, and click the **Tools & Drivers** tab on the VMware Workstation download page.

NOTE If instead of creating a movie you want to actually record the activity of the virtual machine, see [Chapter 13, “Recording and Replaying Virtual Machine Activity,”](#) on page 233. You might want to record a virtual machine for debugging purposes or to exactly reproduce the steps that cause a certain behavior.

To create and play back a movie of virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered on.
- 3 Choose **VM > Capture Movie**.
A Save File dialog box appears.
- 4 Enter information for your movie and click **Save**.

Use the following guidelines:

- The **Quality** setting determines the compression and therefore the file size of the resulting movie.
- If you select **Omit frames in which nothing occurs**, the movie includes only those periods of time when something is actually happening in the virtual machine. This reduces the file size and length of the movie.

While movie capture is active, a red circle (a virtual LED) appears in the notification area of the window.



- 5 In the virtual machine, perform the actions you want to have appear in the movie.
- 6 To stop the movie, choose **VM > Stop Movie Capture**.

If you do not want to use the menu bar or if you are using the virtual machine in full screen mode, you can right-click the movie capture icon and choose **Stop Movie Capture**. This icon is located in the notification area of the taskbar. The red circle disappears, and the movie is saved.

Workstation saves this image as an `.avi` file on the host.

- 7 Play the movie back in any compatible media player.

Advanced Options for Application Developers

Application developers can use the following APIs, SDKs, and IDEs when writing and debugging applications that run in virtual machines:

- **VIX API for writing programs to automate virtual machine operations** – The API is high-level, easy to use, and practical for both script writers and application programmers. API functions allow you to register, power on or off virtual machines, and run programs in the guest operating systems. There are additional language bindings for Perl, COM, and shell scripts (`vmrun`). For more information, see the VMware VIX API Release Notes.
- **VAssert API for inserting replay-only code to debug applications** – Use virtual assertions as you would regular assertions in the applications you develop. The benefit of VAsserts is that they appear only when you replay a recording of using the application and so are overhead-free. Currently available for Windows guests. See the *VAssert Programming Guide*.
- **VProbes tool for investigating guest behavior** – You can write VProbes scripts that inspect and record activities in the guest, VMM, VMX, and virtual device state, without modifying that state. For example, VProbes can track which applications are running or indicate which processes are causing page faults. See the *VProbes Reference Guide*.
- **Visual Studio and Eclipse Integrated Virtual Debuggers** – With the Workstation IDE (integrated development environment) plug-ins, you have a configurable interface between virtual machines and Visual Studio (Windows only) or Eclipse (Windows or Linux) that lets you easily test, run, and debug programs in virtual machines. See [Appendix B, “Using the Eclipse Integrated Virtual Debugger,”](#) on page 463 and [Appendix C, “Using the Visual Studio Integrated Virtual Debugger,”](#) on page 475.

BETA

Transferring Files and Text Between the Host and Guest

9

This chapter discusses how to transfer files between the host and guest. This chapter includes the following topics:

- [“Using Drag-and-Drop”](#) on page 175
- [“Using Copy and Paste”](#) on page 176
- [“Using Shared Folders”](#) on page 177
- [“Using a Mapped Drive for Windows Only”](#) on page 184

Using Drag-and-Drop

To use the drag-and-drop feature, VMware Tools must be installed on the virtual machine. This feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome. With this feature, you can move files and directories easily between Linux and Windows hosts and Linux, Windows, and Solaris 10 guests. However, the drag-and-drop feature does not work on Windows 95 and Windows 98 guests.

You can drag-and-drop files or folders from the following locations:

- A file manager, such as Windows Explorer, on the host to a file manager in the virtual machine and the reverse.
- A file manager to an application that supports drag-and-drop.
- Applications such as zip file managers that support drag-and-drop extraction of individual files.
- One virtual machine to another.

When you drag a file or folder from host to virtual machine or the reverse, Workstation copies the file or folder to the location where you drop it. For example, if you drop a file on the desktop icon of a word processor, the word processor opens with a copy of the original file. The original file does not reflect any changes you make to the copy.

Initially, the application opens using a copy of the file that is stored in your temp directory. On Windows, this is the file specified in the %TEMP% environment variable, and on Linux and Solaris, it is the /tmp/VMwareDnD directory. To protect any changes you make, choose **File > Save As** from the application's menu and save the file in a different directory.

Enable or Disable Drag-and-Drop

To prevent files from being transferred between the virtual machine and the host, disable the drag-and-drop feature. Before you begin, make sure VMware Tools is installed on the virtual machine.

To enable or disable drag-and-drop for a virtual machine

- 1 Start Workstation and select the virtual machine.
The virtual machine can be either powered on or powered off.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 Click the **Options** tab and select **Guest Isolation**.
- 4 Select or deselect the **Enable drag and drop to and from this virtual machine** check box and click **OK**.

Using Copy and Paste

To use the copy and paste feature, VMware Tools must be installed on the virtual machine. This feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome. Copying and pasting text and files works with Linux and Windows hosts and Linux, Windows, and Solaris 10 guests. However, this feature does not work on Windows 95, 98, and NT guests.

You can cut or copy and paste text from one virtual machine to another, but you cannot copy and paste files between virtual machines. You can cut or copy and paste text between applications in the virtual machine and the host computer or between two virtual machines. Use the normal hot keys or menu choices to cut or copy and paste.

Enable or Disable Copy and Paste

To prevent accidental copying and pasting from one environment to another, disable this feature. Before you begin, VMware Tools must be installed on the virtual machine and it is powered off.

To enable or disable copy and paste

- 1 Select the virtual machine.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 Click the **Options** tab, and select **Guest Isolation**.
- 4 Select or deselect the **Enable copy and paste to and from virtual machine** check box and click **OK**.

Using Shared Folders

With shared folders you can share files among virtual machines and the host computer. You choose a directory on the host or on a network directory that is accessible to the host, and you give it the name you want to use on the guest.

To use shared folders, the current version of VMware Tools must be installed in the guest operating system and the virtual machine settings must specify which directories are to be shared. The shared folders can be in the host computer's file system or they can be network directories accessible from the host computer.

You can use shared folders with virtual machines running the following guest operating systems and on all supported host systems:

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0
- Windows Vista
- Linux with a kernel version of 2.4 or higher
- Solaris x86 10
- Solaris x86 10 Update 1
- Solaris x86 10 Update 2
- Solaris x86 10 Update 3

Set Up Shared Folders

To set up shared folders

- 1 Start Workstation and select a virtual machine.

The virtual machine can be either powered on or powered off.

- 2 Choose **VM > Settings**.

The virtual machine settings editor opens.

- 3 Click the **Options** tab and select **Shared Folders**.

- 4 Click **Add**.

On Windows, clicking **Add** starts the Add Shared Folder wizard. On Linux, it opens the Shared Folder Properties dialog box.

- 5 Use the following information to complete the wizard or Properties dialog box:

- **Name** – Name that appears inside the virtual machine.
- **Host folder** – Path on the host to the directory that you want to share.

If you specify a directory on a network share, such as D:\share, Workstation always attempts to use that path. If the directory is later connected to the host on a different drive letter, the shared folder cannot be located.
- **Enabled** or **Enable this share** – Deselect this option to disable a shared folder without deleting it from the virtual machine configuration. You can enable the folder by selecting the check box next to its name in the list.

To enable a folder at a later time select its name in the list, click **Properties**, and enable the folder in the Properties dialog box.
- **Read-only** – Select this option to prevent the virtual machine from changing the contents of the shared folder in the host file system. Access to files in the shared folder is also governed by permission settings on the host computer.

To change these properties, use the Properties dialog box. On Windows, after you select **Shared Folders** on the **Options** tab, click **Properties**.

- 6 (Optional) To enable shared folders for a virtual machine after a shared folder is created, on the **Shared Folders** settings panel, use one of the check boxes in the **Folder Sharing** section:
 - Select **Enabled until next power off or suspend** to enable folder sharing temporarily, until you power off or suspend the virtual machine.

If you select **Enabled until next power off or suspend** and restart the guest or use the guest operating system to shut down, shared folders are not disabled when you restart the virtual machine.

- Select **Always enabled** to enable or disable specific folders in the **Folders** section.
- 7 Access the enabled shared folder on the guest operating system:
- On a Windows guest operating system, map a network drive to the Shared Folders directory, as described in [“Viewing a Shared Folder”](#) on page 181.
 - On Linux, shared folders appear under `/mnt/hgfs`.
 - On Solaris, shared folders appear under `/hgfs`.

Enabling and Disabling Shared Folders

A shared folder is disabled by default if it was not created by the user that powers on the virtual machine. This is a security precaution. The following sections describe how to enable shared folders for virtual machines created by other users, enable or disable folder sharing for a specific virtual machine, and enable a specific shared folder for a virtual machine.



CAUTION Enabling all shared folders can pose a security risk because a shared folder might enable existing programs inside the virtual machine to access the host file system without your knowledge.

You can enable folder sharing if you created virtual machines with Workstation 4, 5, or 6. Folder sharing for Workstation 4, 5, and 6 virtual machines is also disabled by default.

To avoid the security threat of enabling all shared folders, you must first enable folder sharing for a specific virtual machine and then enable a specific shared folder. This is because after you enable folder sharing for a virtual machine, you cannot share particular folders unless the specific folders are also enabled.

On Windows, if you disable shared folders, after you power on a virtual machine and attempt to select a mapped drive to the shared folder, you receive a message that the connection cannot be made.

Enable Shared Folders for Virtual Machines Created By Other Users

To enable shared folders for virtual machines created by other users

- 1 From the **Workstation** menu bar, choose **Edit > Preferences**.
- 2 On the **Workspace** tab, in the **Virtual Machines** section, select **Enable all shared folders by default**.

This setting applies to shared folders on all virtual machines that are created by other users, such as appliance developers.

Enable or Disable Shared Folders for Specific Virtual Machines

To enable or disable shared folders for specific virtual machines

- 1 Select a virtual machine.
The virtual machine can be powered off or powered on.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 Click the **Options** tab and select **Shared Folders**.
- 4 Use the check boxes in the **Folder Sharing** section to enable or disable shared folders and click **OK**.

Turn the virtual machine on and select **Enabled until next power off or suspend** to enable folder sharing temporarily, until you shut down, suspend, or restart the virtual machine. You must select this option or **Always enabled** to enable or disable specific folders in the **Folders** section.

Enable Specific Shared Folders for a Virtual Machine

To enable specific shared folders for a virtual machine

- 1 Select the virtual machine.
The virtual machine can be either powered on or powered off.
- 2 Choose **VM > Settings > Options > Shared Folders**.
- 3 In the **Folders** list for the virtual machine, select the check box next to the name of the shared folder that you want to enable.
- 4 (Optional) To make the shared folder read-only, select the shared folder and click **Properties**, select the read-only check box and click **OK**.

Viewing a Shared Folder

Viewing shared folders varies based on the guest operating system. The following sections describe viewing shared folders in Windows, Solaris, and Linux guests. You can use shared folders to share any type of files.



CAUTION Do not open a file in a shared folder from more than one application at a time. For example, do not open the same file using an application on the host operating system and another application in the guest operating system. If one of the applications writes to the file, data corruption can occur.

View and Map Shared Folders in a Windows Guest

In a Windows guest operating system, you can view shared folders using desktop icons.

NOTE If your guest operating system has VMware Tools from Workstation 4.0, shared folders appear as folders on a designated drive letter.

To view shared folders in a Windows guest

- Look in **My Network Places > Entire Network** (**Network Neighborhood** for a Windows NT guest, or **Network** for Windows Vista) under **VMware Shared Folders**.

If you have trouble finding a shared folder using the desktop icon, open Windows Explorer and look in **My Network Places** (or **Network Neighborhood**).

- To view a specific shared folder, do one of the following:
 - Navigate to it on the guest system by opening **My Network Places > Entire Network > VMware Shared Folders > .host > Shared Folders > <shared_folder_name>**.
 - Go directly to the folder using the UNC path `\\.\host\Shared Folders\<shared_folder_name>`.
- To map a shared folder to a drive letter on the guest system do one of the following:
 - In Windows Explorer, choose **Tools > Map Network Drive** and browse to the location of the shared folder.
 - Go directly to the folder using the UNC path `\\.\host\Shared Folders`.

View Shared Folders in a Linux or Solaris 10 Guest

To view shared folders in a Linux or Solaris 10 guest

- On a Linux virtual machine, shared folders appear under `/mnt/hgfs`.
- On a Solaris virtual machine, shared folders appear under `/hgfs`.

View Shared Folders on the Host

From the Workstation menu bar, choose **VM > Settings > Options > Shared Folders** to see a list of the shared folders and the directory paths to them.

Permissions and Folder Mounting for Shared Folders on Linux Guests

The version of VMware Tools included in Workstation 6.5 contains performance improvements, support for symbolic links if you use a Linux host, a new mechanism for mounting shared folders, and permissions enhancements.

Performance Improvements

Host-guest file sharing is integrated with the guest page cache. Files in shared folders are cached for reading and can be written to asynchronously. However, you do not experience the read caching benefits on files that are being actively written to from the guest.

To speed performance, use the `ttl` (time to live) option to the `mount` command. Use this option to specify the interval used by the `hgfs` (host-guest file system) driver for validating file attributes. For example, if you use the following command, attributes are validated every 3 seconds instead of every 1 second, which is the default:

```
mount -o ttl=3 -t vmhgfs .host:/<share> <mountpoint>
```

NOTE Lengthening the interval involves some risk. If something in the host modifies a file's attributes, the guest might not get the modifications as quickly, and the file can become corrupted.

Folder Mounting

This mechanism allows you to mount one or more directories or subdirectories in a shared folder to any location in your file system in addition to the default location of `/mnt/hgfs`. You can use the `mount` program to mount all shares, one share, or a subdirectory within a share to any location in your file system, for example:

```
mount -t vmhgfs .host:/ /home/user1/shares
```

mounts all shares to `/home/user1/shares`.

```
mount -t vmhgfs .host:/foo /tmp/foo
```

mounts the share named `foo` to `/tmp/foo`.

```
mount -t vmhgfs .host:/foo/bar /var/lib/bar
```

mounts the subdirectory `bar` within the share `foo` to `/var/lib/bar`.

When you use the `mount` program, you can use VMware-specific options in addition to the standard `mount` syntax. To see usage information host-guest file system options, enter this command:

```
/sbin/mount.vmhgfs -h
```

NOTE When you install VMware Tools, an entry is made to `etc/fstab` to specify the location of shared folders. You can edit this file to change or add entries.

To use `mount` in this way, you must use the virtual machine settings editor in Workstation to set up and enable a shared folder. After the share exists, you can mount it to other locations besides the default.

In previous versions of VMware Tools, when a Linux guest attempted to mount a shared folder, the `vmware-guestd` program attempted to perform the mount. If it failed, the only evidence of the failure was an empty folder.

With the new version of VMware Tools, the Tools services script loads a driver that performs the mount. If the mount fails, a message appears regarding mounting HGFS shares.

The mount can fail if shared folders are disabled or if the share does not exist. You are not prompted to re-run the VMware Tools configurator (the `vmware-config-tools.pl` file).

Improved Handling of Permissions

Many refinements have been made for Linux guests on both Linux and Windows hosts:

- If you use a Linux host and create files that you want to share with a Linux guest, the file permissions shown on the guest are exactly the same as those on the host.

Use `fmask` and `dmask` to mask permissions bits for files and directories.

- If you use a Windows host and create files that you want to share with a Linux guest, read-only files are displayed as having read and execute permission for everyone, and other files are shown as fully writable by everyone.
- If you use a Linux guest to create files for which you want to restrict permissions, use the `mount` program with the following options in the guest: `uid`, `gid`, `fmask`, `dmask`, `ro` (read-only), and `rw` (read-write). Note that `rw` is the default.

If you are using a Windows host or a Linux host created with a previous release of Workstation, you can change only the owner permissions. This behavior is the same as in previous releases.

Using a Mapped Drive for Windows Only

You can map a virtual disk to a host instead of using shared folders or copying data between a Windows guest and host. In this case, you can mount a virtual disk in a Windows host file system as a separate mapped drive. Using a mapped drive lets you connect to the virtual disk without going into a virtual machine.

After you map a drive to the virtual disk, you are not able to power on any virtual machine that uses that disk until you disconnect it from the host. Map only disks for Windows guests. If you map a disk from a Linux guest, when you attempt to access the disk from your host computer, you are prompted to format the disk.

You can use Workstation to map the disk to a drive on the host, and to disconnect the drive. If you attempt to use the host's **My Computer > Tools > Disconnect Network Drive** command, you are not see the mapped drive letter in the list of network drives.

NOTE You can mount volumes (partitions) formatted with FAT (12/16/32) or NTFS only. You cannot mount a virtual disk if any of its `.vmdk` files are compressed or have read-only permissions.

Map a Virtual Disk to a Drive on the Host

Before you begin to map a virtual disk, make sure that all virtual machines that use the disk are powered off.



CAUTION VMware recommends that you leave the check box called **Open file in read-only mode** selected in the Map a Virtual Disk dialog box. This setting prevents you from accidentally writing data to a virtual disk that might be the parent of a snapshot or linked clone. Writing to such a disk might make the snapshot or clone unusable.

To map a virtual disk to a drive on the host

- 1 Choose **File > Map or Disconnect Virtual Disks**.
- 2 In the Map or Disconnect Virtual Drives dialog box, click **Map**.
- 3 In the dialog box that appears, click **Browse**, navigate to a disk file (.vmdk file) select it, and click **Open**.

You are returned to the Map a Virtual Disk dialog box.

- 4 Select the volume to map, and select a drive letter that is not being used on your host.
- 5 Click **OK**.
The drive appears in Windows Explorer on your host. From the host, you can read from or write to files on the mapped virtual disk.
- 6 (Optional) To view mapped drive, choose **VM > Settings > Hardware**, select the hard disk and click **Utilities > Map**.

The Map Virtual Disk dialog box appears with the corresponding .vmdk file already selected.

Disconnect the Host from the Virtual Disk

To access the mapped virtual disk from a virtual machine again, you must disconnect it. You can disconnect the host from the virtual disk using two different methods.

To disconnect the host from the virtual disk

- 1 Choose **File > Map or Disconnect Virtual Disks**.
- 2 In the Map or Disconnect Virtual Drives dialog box, select a volume to disconnect and click **Disconnect**.

- 3 If you receive an error message asking whether to forcibly disconnect, click **Yes**.
- 4 Click **OK**.
- 5 (Optional) To view mapped drive, choose **VM > Settings > Hardware**, select the hard disk and click **Utilities > Disconnect**.

You can now power on any virtual machine that uses this disk.

BETA

Preserving the State of a Virtual Machine

10

Suspending a virtual machine lets you save the current state so that you can continue work later from the same state. Taking a snapshot lets you preserve the state of the virtual machine so you can return to the same state repeatedly. This chapter includes the following topics:

- [“Using the Suspend and Resume Features”](#) on page 187
- [“Using Snapshots”](#) on page 189

Using the Suspend and Resume Features

You can use the suspend and resume features to save the current state of a virtual machine. When you resume, any applications you were running when you suspended the virtual machine are resumed in their running state, and the content is the same as when you suspended the virtual machine.

The speed of the suspend and resume operations depends on how much data changed during the time that the virtual machine was running. In general, the first suspend operation takes longer than later suspend operations.

When you resume and do additional work in the virtual machine, you cannot return to the state the virtual machine was in at the time you suspended. To preserve the state of the virtual machine so that you can return to the same state repeatedly take a snapshot, as described in [“Using Snapshots”](#) on page 189.

Use Hard Suspend or Soft Suspend

You can configure the **Suspend** button or menu command to run a VMware Tools script in the guest operating system before doing the suspend operation. This configuration is called a soft suspend.

Before you begin, make sure VMware Tools is installed in the guest operating system. See [“Installing VMware Tools”](#) on page 105.

On Windows guests, when you do a soft suspend, a script releases the IP address if the guest operating system is using DHCP. On Linux, FreeBSD, and Solaris guests, the script stops networking for the virtual machine. When you use the **Resume** command on Windows guests, a script gets a new IP address from DHCP. On Linux, FreeBSD, and Solaris guests, networking restarts.

To use hard suspend or soft suspend

- 1 Select the virtual machine and choose **VM > Settings** from the Workstation menu bar.

The virtual machine can be either powered off or on. The virtual machine settings editor opens.
- 2 Click the **Options** tab, and select **Power**.
- 3 In the **Power controls** section, specify a hard suspend (**Suspend**) or a soft suspend (**Suspend Guest**) operation.
- 4 Click **OK**.

Suspend or Resume a Virtual Machine

The suspend and resume features let you save the current state of your virtual machine and continue work later from the same state.

Before suspending a virtual machine, specify whether to stop networking before suspending. See [“Use Hard Suspend or Soft Suspend”](#) on page 187.

To suspend or resume a virtual machine

Do one of the following:

- To suspend a virtual machine, choose **VM > Power > Suspend**.

If your virtual machine is running in full screen mode, which hides the toolbar, return to windowed mode. by pressing the Ctrl+Alt+Enter key combination.

When you suspend a virtual machine, a file with a `.vmss` extension is created in the working directory. This file contains the entire state of the virtual machine. See [“Virtual Machine Location”](#) on page 88.

- To resume a suspended virtual machine that you suspended, select the virtual machine and choose **VM > Power > Suspend**.

When you resume the virtual machine, its state is restored from the `.vmss` file.

Using Snapshots

Taking snapshots lets you preserve the state of the virtual machine so that you can return to the same state repeatedly.

Scenarios for Using Multiple Snapshots

You can take multiple snapshots of a virtual machine.

Snapshots in a Linear Process

Taking snapshots in a linear process means taking a snapshot, continuing to use the virtual machine from that point, taking another snapshot at a later point, and so on. Each snapshot is a restoration point in a single long sequence.

Figure 10-1. Snapshots as Restoration Points in a Linear Process



Workstation supports more than 100 snapshots for each linear process.

Use snapshots in a linear process for the following situations:

- You plan to make risky changes in a virtual machine, such as by testing new software or examining a virus. Before adding new, untested code to a project, take a snapshot.

You can always revert to a previous known working state of the project if the new code does not work as expected. If the new code causes no problems, you can take another snapshot of the virtual machine in its new state.

NOTE You can configure a virtual machine to take a snapshot any time it is powered off, preserving a virtual audit trail as work progresses. See [“Take or Revert to a Snapshot at Power Off”](#) on page 197.

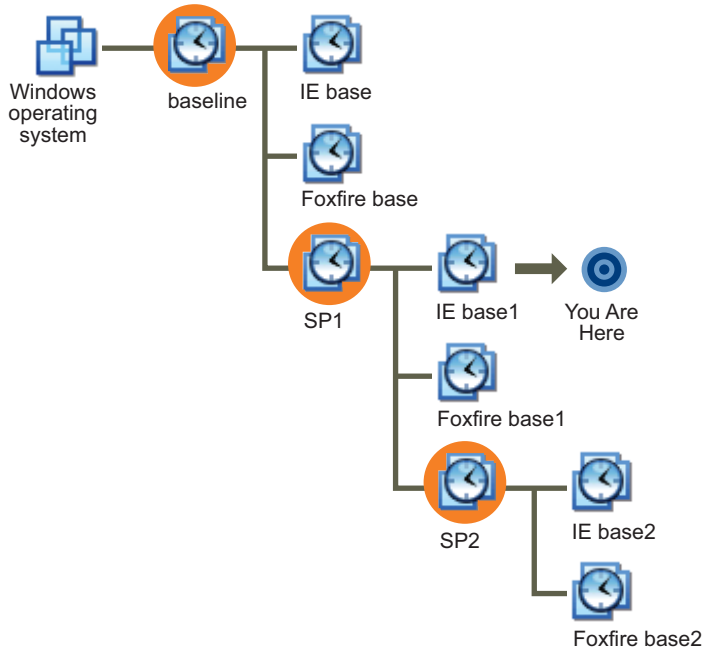
- You create a training course and want to save the state of the virtual machine in a snapshot at each lesson’s starting point. You can use the snapshots to skip lengthy computer preparation time.

You can also configure the virtual machine to revert to a snapshot any time it is powered off. Each time a new class begins a lesson, the previous student’s work is discarded. See [“Revert at Power Off”](#) on page 196.

Snapshots in a Process Tree

You can save a number of sequences as branches from a single baseline, as [Figure 10-2](#) shows. This strategy is often used in testing software. You can take a snapshot before installing different versions of a program to ensure that each installation begins from an identical baseline.

Figure 10-2. Snapshots as Restoration Points in a Process Tree



Workstation supports more than 100 snapshots for each branch in a process tree.

Snapshot Relationships

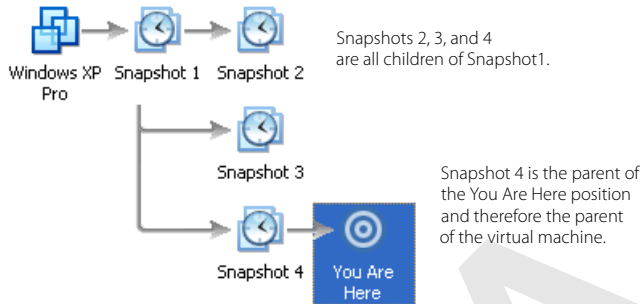
The relationship between snapshots is like a parent-child relationship:

- In a linear process, each snapshot has one parent and one child, except for the last snapshot, which has no children.
- In a process tree, each snapshot has one parent, but one snapshot can have more than one child. Many snapshots have no children.

The parent snapshot of a virtual machine is the snapshot on which the current state (the You Are Here position in [Figure 10-3](#)) is based. After you take a snapshot, that stored

state is the parent snapshot of the virtual machine. If you revert or go to an earlier snapshot, the earlier snapshot becomes the parent snapshot of the virtual machine.

Figure 10-3. Parent-Child Relationship Between Snapshots



Information Captured by Snapshots

A snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes:

- **Memory state** – Contents of the virtual machine memory
- **Settings state** – Virtual machine settings
- **Disk state** – State of all the virtual disks

The state of a physical disk or independent disk is not preserved when you take a snapshot.

Snapshots operate on individual virtual machines. If you select a team of virtual machines and take a snapshot, only the state of the active virtual machine is preserved. See [“Summary and Console Views for Teams and Their Virtual Machines”](#) on page 249.

When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot. To suspend, power on, or power off the virtual machine when you launch it, be sure it is in that state when you take the snapshot.

Snapshot Conflicts

Avoid taking a snapshot when applications in the virtual machine are communicating with other computers, especially in production environments.

Suppose you take a snapshot while the virtual machine is downloading a file from a server on the network. After you take the snapshot, the virtual machine continues downloading the file, communicating its progress to the server. If you revert to the

snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Or consider a case in which you take a snapshot while an application in the virtual machine is sending a transaction to a database on a separate machine. If you revert to that snapshot after the transaction starts but before it is committed, the database is likely to be confused.

Enable or Disable Background Snapshots

When you set a preference to take snapshots in the background, you can continue working while the state of the virtual machine is being preserved.

If you take another snapshot or revert to a snapshot before Workstation completes a pending snapshot operation, a progress dialog box appears. You must wait for the pending snapshot operation to finish before the next snapshot or resume operation begins.

Enabling background snapshots for a host with slow hard disks can adversely affect performance. If you experience significant performance problems when taking or restoring snapshots, disable background snapshots.

To enable or disable background snapshots

- 1 From the Workstation menu bar, choose **Edit > Preferences**.
- 2 Click the **Priority** tab and do one of the following:
 - To enable background snapshots, select the check box in the **Snapshots** section.
 - To disable background snapshots, deselect the check box.
- 3 Click **OK** and restart the virtual machine.

Exclude a Virtual Disk from Snapshots

In certain configurations, you might want to revert some disks to a snapshot while other disks retain all changes. For example, you might want a snapshot to preserve a disk with your operating system and applications, while always keeping the changes to a disk with your documents.

You can exclude virtual disks from a snapshot by changing the disk mode. Before you begin, power off the virtual machine and delete any existing snapshots.

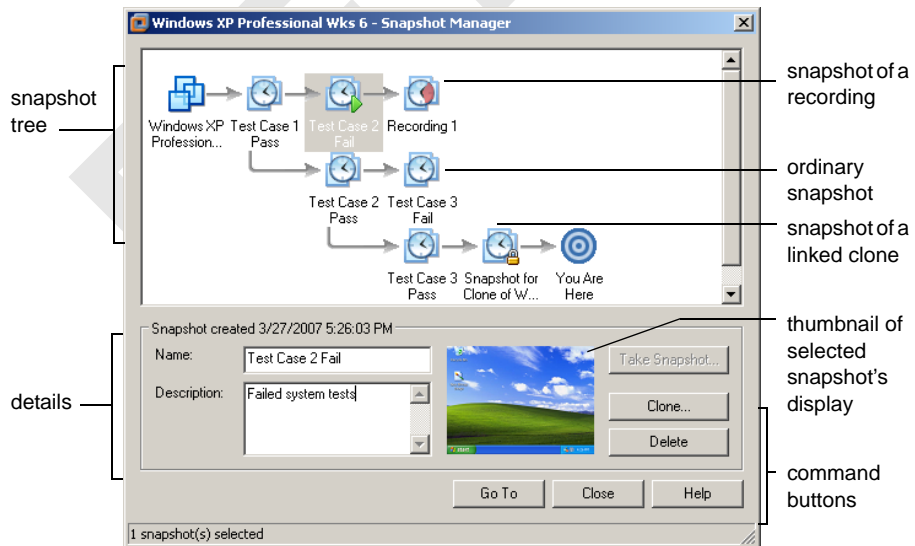
To exclude a virtual disk from snapshots

- 1 Start Workstation and select the virtual machine.
- 2 Choose **VM > Settings**.
- 3 On the **Hardware** tab, select the drive to exclude and click **Advanced**.
- 4 Select **Independent** and select one of the following options:
 - **Persistent** – Changes are immediately and permanently written to the disk. All changes to an independent disk in persistent mode remain, even when you revert to a snapshot.
 - **Nonpersistent** – Current changes to the disk are discarded when you power off or revert to a snapshot.

Snapshot Manager Overview

You can review all snapshots for the active virtual machine and act on them directly in the snapshot manager. [Figure 10-4](#) illustrates the components of the snapshot manager.

Figure 10-4. Snapshot Manager on a Windows Host



The snapshot tree shows all snapshots for the virtual machine and the relationship between snapshots. The **You Are Here** icon is not a snapshot. It shows the current state of the virtual machine. See [“Snapshot Relationships”](#) on page 190.

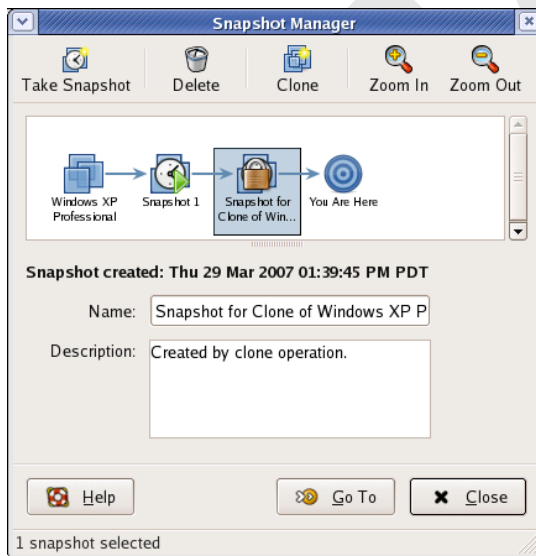
NOTE Point to a snapshot (without clicking) to display the complete name of that snapshot.

Most snapshot manager actions are available as menu commands from the **VM > Snapshot** menu. The following actions, however, are available only from the snapshot manager:

- **Renaming a snapshot** – The **Name** text box is editable. If you rename a snapshot for a cloned virtual machine, use the **Description** field for future identification.
- **Changing or adding a description** – The **Description** text box is editable.
- **Deleting a snapshot** – See [“Delete a Snapshot or a Recording”](#) on page 197.

The snapshot manager has a slightly different appearance on Linux hosts, as shown in [Figure 10-5](#).

Figure 10-5. Snapshot Manager on a Linux Host



On Linux hosts, right-click the toolbar to change the icon style. You can display icons and text, icons only, text only, and so on.

Open and Use the Snapshot Manager

Use the snapshot manager to review all snapshots for the active virtual machine and act on them directly.

To open and use the snapshot manager

- 1 From the Workstation menu bar, choose **VM > Snapshot > Snapshot Manager**.
- 2 Select a snapshot or recording and click the button for the desired action.

To select more than one snapshot or recording, Ctrl+click the desired snapshots and recordings.

If the **Take Snapshot** button is disabled, it might be because the virtual machine has multiple disks in different disk modes. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.

Take a Snapshot

You can usually take a snapshot while a virtual machine is powered on, powered off, or suspended.

Following are the prerequisites for taking a snapshot:

- Any suspend operations must be complete.
- The virtual machine is not communicating with another computer. See [“Snapshot Conflicts”](#) on page 191.
- If your use of virtual machines is strongly performance oriented, the guest operating system’s drives are defragmented. See [“Defragment Virtual Disks”](#) on page 217.
- If the virtual machine has multiple disks in different disk modes, the virtual machine is powered off. For example, if a special purpose configuration requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- If the virtual machine was created with Workstation 4 delete any existing snapshots or upgrade the virtual machine to Workstation 5 or higher. See [“Change the Version of the Virtual Machine”](#) on page 57.

To take a snapshot

- 1 Choose **VM > Snapshot > Take Snapshot**.
- 2 Enter a unique name.
- 3 (Optional) Enter a description.

Use this field to record notes about the virtual machine state captured in the snapshot.

- 4 Click **OK**.

Rename a Snapshot or Recording

Use the snapshot manager to change the name of a snapshot or its description at any time.

To rename a snapshot or recording

- 1 From the Workstation menu bar, choose **VM > Snapshot > Snapshot Manager**.
- 2 Select the snapshot or recording.
- 3 Edit the text in the **Name** text box and click **Close**.

If you rename a snapshot for a cloned virtual machine, use the **Description** field to specify which virtual machine was cloned.

Restore an Earlier State from a Snapshot

Restore a snapshot in Workstation by using the **Revert** and **Go to** commands.

The **Revert** command has the same effect as using the **Go to** command and selecting the parent snapshot of the virtual machine. It reverts to the parent snapshot of the current state. This state corresponds to the You Are Here position in the snapshot manager. See [“Snapshot Relationships”](#) on page 190.

The **Go to** command is not limited to the parent snapshot of the current state. You can choose any existing snapshot of the virtual machine.

To restore an earlier state from a snapshot

Do one of the following:

- To revert to the parent snapshot, choose **VM > Snapshot > Revert to Snapshot**.
- To revert to a snapshot that is not the parent, choose **VM > Snapshot** and select the snapshot name.
- To set the virtual machine to revert to the parent snapshot every time the virtual machine is powered off, see [“Revert at Power Off”](#) on page 196.

Revert at Power Off

You can set the virtual machine to revert to the parent snapshot any time it is powered off. The parent snapshot of a virtual machine is the snapshot on which the current state (the You Are Here position) is based.

To set a virtual machine to revert to a snapshot at power off

- 1 Start Workstation and select the virtual machine.
The virtual machine can be either powered on or powered off.
- 2 Choose **VM > Settings**.
- 3 Click the **Options** tab and select **Snapshot/Replay**.
- 4 In the **When powering off** section, select **Revert to snapshot**.

Delete a Snapshot or a Recording

Deleting a snapshot or recording does not affect other snapshots, recordings, or the current state of the virtual machine. Use the snapshot manager to delete a snapshot.



CAUTION If a snapshot is used to create a clone, the snapshot becomes locked. If you delete a locked snapshot, the clones created from that snapshot no longer operate.

You cannot delete a snapshot if the associated virtual machine is designated as a template for cloning. See [“Enable Template Mode for a Parent Virtual Machine of Linked Clones”](#) on page 203

To delete a snapshot or recording

- 1 Choose **VM > Snapshot > Snapshot Manager**.
- 2 Do one of the following:
 - To delete a single snapshot or recording, select it and click **Delete**.
 - To delete a snapshot or recording and all its children, right-click it and choose **Delete Snapshot/Recording and Children**.
 - To delete all snapshots and recordings, right-click a snapshot or recording, choose **Select All**, and click **Delete**.
- 3 When prompted to confirm the deletion, click **OK**, and click **Close** in the snapshot manager.

Take or Revert to a Snapshot at Power Off

You can set a virtual machine to automatically revert to a snapshot or to take a new snapshot whenever you power off the virtual machine.

To take a snapshot or revert to one at power off

- 1 Select the virtual machine.

The virtual machine can be either powered on or powered off.

- 2 Choose **VM > Settings**.

The virtual machine settings editor opens.

- 3 Click the **Options** tab and select **Snapshot/Replay**.

- 4 Select an option in the **When powering off** section:

- **Just power off** – Powers off without making any changes to snapshots.
- **Revert to snapshot** – Reverts to the parent snapshot of the current state of the virtual machine (that is, the parent snapshot of the You Are Here position in the Snapshot Manager window).
- An instructor might use this setting to discard student answers for a computer lesson when a virtual machine is powered off at the end of class.
- **Take a new snapshot** – Takes a snapshot of the virtual machine state after it is powered off. This is useful to preserve milestones automatically. The snapshot appears in the snapshot manager. The name of this snapshot is the date and time the virtual machine was powered off. The description is “Automatic snapshot created when powering off.”
- **Ask me** – Prompts you, every time you power off a virtual machine, choose to power off, revert, or take a snapshot.

- 5 Click **OK**.

Snapshots and Workstation 4 Virtual Machines

Workstation 4 virtual machines do not support multiple snapshots. For full Workstation 6 functionality, you must upgrade. See [“Change the Version of the Virtual Machine”](#) on page 57.

If your Workstation 4 virtual machine has a snapshot, you must remove the snapshot before you upgrade. Use your earlier, Workstation 4 application to remove the snapshot, and then upgrade to Workstation 6.

Cloning, Moving, and Sharing Virtual Machines

11

Cloning a virtual machine is faster and easier than copying it. This chapter provides instructions and also provides information on how to move your virtual machines from one host to another, or elsewhere on the same host, plus recommendations on how to share virtual machines with other users. This chapter includes the following topics:

- [“The Virtual Machine’s Universal Unique Identifier”](#) on page 199
- [“Cloning a Virtual Machine”](#) on page 201
- [“Moving a Virtual Machine”](#) on page 205
- [“Moving an Older Virtual Machine”](#) on page 209
- [“Moving Linked Clones”](#) on page 209
- [“Sharing Virtual Machines with Other Users”](#) on page 209
- [“Sharing Virtual Machines with VMware Player”](#) on page 210

The Virtual Machine’s Universal Unique Identifier

To ensure all virtual machines are identified properly, each virtual machine is automatically assigned a universal unique identifier (UUID).

Use the UUID of a virtual machine for system management in the same way you use the UUID of a physical computer. The UUID is stored in the SMBIOS system information descriptor. It can be accessed by standard SMBIOS scanning software, such as SiSoftware Sandra or the IBM utility `smbios2`.

This UUID is generated when you initially power on the virtual machine. As long as you do not move or copy the virtual machine to another location, the UUID remains constant. To set a specific UUID, see [“Specify a UUID for a Virtual Machine”](#) on page 201.

UUID Options When You Move a Virtual Machine

When you power on a virtual machine that was moved or copied to a new location, the following message appears:

The virtual machine's configuration file has changed its location since its last power-on. Do you want to create a new unique identifier (UUID) for the virtual machine, or keep the old one?

Which of the following options you choose depends on the cause of the changed UUID:

- **Keep** – If the virtual machine was moved rather than copied, you can choose to keep the UUID.
- **Create** – If the virtual machine was copied to a new location, create a new UUID so that the copy has its own UUID that does not conflict with the original virtual machine. If you are not sure which option to choose, the safest option is **Create**.
- **Always Create** – If the original virtual machine is being used as a master copy for more virtual machines, you can create a new UUID the first time you power on each copy. After you configure the virtual machine and are ready to make it a master copy, move it to a new location and power it on. When the message appears after you power on, select **Always Create**. The virtual machine is set up to create a new UUID every time it is moved. Power off the virtual machine and begin using it as a master copy by copying the virtual machine files to other locations.

NOTE You can avoid creating a master copy that always creates a new UUID if you simply clone the virtual machine rather than copy it. See [“Cloning a Virtual Machine”](#) on page 201.

- **Always Keep** – If you intend to move the virtual machine numerous times and want to keep the same UUID each time the virtual machine moves, select **Always Keep**.

NOTE To change the **Always Keep** or **Always Create** setting, power off the virtual machine and edit its configuration file (.vmx). Delete the line that contains this text:

```
uuid.action = "create"
```

or

```
uuid.action = "keep"
```

Conversely, to specify to always keep or always create the UUID and not prompt the user to choose a setting when first powering on the virtual machine, edit the configuration file and add the appropriate line for `uuid.action`.

Suspending and resuming a virtual machine does not trigger the process that generates a UUID. The UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it was copied or moved. The next time the virtual machine is rebooted, the message appears, so you can create a new UUID or keep the existing one.

Specify a UUID for a Virtual Machine

Although UUIDs are automatically assigned to virtual machines, you can override the generated UUID value and assign a specific UUID.

The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces, except for a dash between the eighth and ninth hexadecimal pairs. Following is an example of a UUID:

```
00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff
```

To specify a UUID for a virtual machine

- 1 Power off the virtual machine.
- 2 Open the configuration (.vmx) file with a text editor.
- 3 Search for the line that contains `uuid.bios`.

The format of the line is `uuid.bios = "<uuid_value>"`, with quotation marks around the parameter value. Following is an example of the configuration setting:

```
uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
```

- 4 Replace the existing UUID value with the specific UUID value.
- 5 Save and close the file.
- 6 Power on the virtual machine.

The new UUID is used when the virtual machine boots.

Cloning a Virtual Machine

This section provides instructions for creating and configuring clones of virtual machines.

A clone is a copy of an existing virtual machine. The existing virtual machine is called the parent of the clone. When the cloning operation is complete, the clone becomes a separate virtual machine. These are the main characteristics of a clone:

- Changes made to a clone do not affect the parent virtual machine. Changes made to the parent virtual machine do not appear in a clone.

- A clone's MAC address and UUID are different from those of the parent virtual machine.

Make a clone when you need a copy of a virtual machine for separate use. Make a snapshot rather than a clone if you want to save the current state of the virtual machine, so that you can revert to that state.

Although a clone is a separate virtual machine, if the clone is a linked clone, it shares virtual disks with the parent virtual machine. See [“Types of Clones”](#) on page 202.

Uses of a Clone

Installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process.

Clones are useful when you must deploy many identical virtual machines to a group. For example:

- An MIS department can clone a virtual machine for each employee, with a suite of preconfigured office applications.
- A virtual machine can be configured with a complete development environment and then cloned repeatedly as a baseline configuration for software testing.
- A teacher can clone a virtual machine for each student, with all the lessons and labs required for the term.

With clones you can make complete copies of a virtual machine, without browsing a host file system or worrying if you have located all the configuration files.

Types of Clones

Two types of clones are available: full and linked.

Full Clones

A full clone is a complete and independent copy of a virtual machine. It shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

Because a full clone does not share virtual disks with the parent virtual machine, full clones generally perform better than linked clones. However, full clones take longer to create than linked clones. Creating a full clone can take several minutes if the files involved are large.

The full clone duplicates only the state of the virtual machine at the instant of the cloning operation. Thus the full clone does not have access to any snapshots that might exist of the parent virtual machine.

Linked Clones

A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. A linked clone is made from a snapshot of the parent. See [“Scenarios for Using Multiple Snapshots”](#) on page 189. This conserves disk space and allows multiple virtual machines to use the same software installation.



CAUTION You cannot delete the linked clone snapshot without destroying the linked clone. It is safe to delete this snapshot only if you deleted the clone depending on it.

All files available on the parent at the moment of the snapshot continue to remain available to the linked clone. Ongoing changes to the virtual disk of the parent do not affect the linked clone, and changes to the disk of the linked clone do not affect the parent.

A linked clone must have access to the parent. Without access to the parent, you cannot use a linked clone. You can make a linked clone from a linked clone, but keep in mind that the performance of the linked clone degrades. When possible, make a linked clone of the parent virtual machine.

If you make a full clone from a linked clone, however, the full clone is an independent virtual machine that does not require access to the linked clone or its ancestors.

Linked clones are created swiftly, so you can easily create a unique virtual machine for each task. You can also easily share a virtual machine with other users by storing the virtual machine on your local network, where other users can quickly make a linked clone. This facilitates collaboration. For example, a support team can reproduce a bug in a virtual machine, and an engineer can quickly make a linked clone of that virtual machine to work on the bug.

Creating Clones

If you decide to create a linked clone and you want to prevent the parent virtual machine from being accidentally deleted, enable template mode before using the Clone Virtual Machine wizard.

Enable Template Mode for a Parent Virtual Machine of Linked Clones

To prevent anyone from deleting the parent virtual machine for a linked clone, designate the parent as a template. When template mode is enabled, a virtual machine

cannot be deleted or added to a team, and the virtual machine's snapshots cannot be deleted.

To enable template mode for a parent virtual machine of linked clones

- 1 Start Workstation and select the virtual machine to use as a parent of your linked clone.

The virtual machine can be either powered on or powered off.

- 2 Verify that the parent has at least one snapshot.

Open the snapshot manager and create a snapshot if none exists. See [“Snapshot Manager Overview”](#) on page 193.

- 3 Open the virtual machine settings editor by choosing **VM > Settings**.

- 4 Click the **Options** tab, and select **Advanced**.

- 5 In the Settings section, click **Enable Template mode (to be used for cloning)** and click **OK**.

Use the Clone Virtual Machine Wizard

The Clone Virtual Machine wizard guides you through the process of making a clone. You do not need to locate and manually copy the parent virtual machine files.

Before making a linked clone, defragment the guest operating system's drives on the parent virtual machine. Use the tools in the guest operating system to run a defragmentation utility. See [“Defragment Virtual Disks”](#) on page 217.

For more information about how to ensure that a linked clone's parent virtual machine cannot be deleted, see [“Enable Template Mode for a Parent Virtual Machine of Linked Clones”](#) on page 203.

NOTE Workstation 4 virtual machines, and virtual machines created with other VMware products that are compatible with version 4, must be upgraded to at least Workstation version 5 virtual machines before you can clone them. See [“Change the Version of the Virtual Machine”](#) on page 57.

To use the Clone Virtual Machine wizard

- 1 Select the virtual machine.

Make sure the virtual machine is powered off.

- 2 Choose **VM > Clone** to open the Clone Virtual Machine wizard.

- 3 On the Welcome page, click **Next**.

- 4 On the Clone Source page, select the state of the parent from which you want to create a clone and click **Next**.

You can choose to create a clone from the parent's current state or from any existing snapshot of the parent. If you select the current state, Workstation creates a snapshot of the virtual machine before cloning it.

The wizard does not allow you to clone from the current state when template mode is enabled.

- 5 On the Clone Type page, specify whether you want to create a linked clone or a full clone and click **Next**.
- 6 On the Name of the New Virtual Machine page, enter a name and a path for the cloned virtual machine and click **Finish**.

The default name and path are based on the original virtual machine name and location.

The Clone Virtual Machine wizard displays a status page. A full clone can take many minutes to create, depending on the size of the virtual disk that is being duplicated.

- 7 Click **Done** to exit the Clone Virtual Machine wizard.

The Clone Virtual Machine wizard automatically creates a new MAC address and UUID for the clone. Other configuration information is identical to that of the parent virtual machine. For example, a machine's name and static IP address configuration are not altered by the Clone Virtual Machine wizard.

- 8 To prevent conflict with static IP addressing, change the clone's static IP address before the clone connects to the network.

See [“Selecting IP Addresses on a Host-Only Network or NAT Configuration”](#) on page 277.

Moving a Virtual Machine

You can take a virtual machine that was created by using Workstation and move it to a different computer or to a different location on the same computer. You can even move your virtual machine to a host with a different operating system. For example, you can move a virtual machine from a Windows host to a Linux or VMware ESX Server host.

In general, moving a virtual machine means moving the files that make up the virtual machine. The path names for all files associated with a Workstation virtual machine are relative, meaning the path to each file is relative to the virtual machine directory. For

example, if you are in the virtual machine directory, the relative path to the virtual disk file is `<machine_name>.vmdk`.



CAUTION Always make backup copies of all the files in your virtual machine's directory before you start a process like this.

Hosts with Different Hardware

The guest operating system might not work correctly if you move a virtual machine to a host with significant hardware differences, such as from a 64-bit host to a 32-bit host or from a multiprocessor host to a uniprocessor host. This section provides details.

Moving Between 64-Bit and 32-Bit Hosts

You can move a virtual machine from a 32-bit host to a 64-bit host but not from a 64-bit host to a 32-bit host.

NOTE Workstation supports 64-bit guest operating systems only in Workstation versions 5.5 and later, and only on host machines with supported processors. When you power on a virtual machine with a 64-bit guest operating system, Workstation performs an internal check. If the host CPU is not a supported 64-bit processor, you cannot power on the virtual machine. For the list of processors Workstation supports for 64-bit guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the **Help** menu.

Moving Between Multiprocessor and Uniprocessor Hosts

For all supported configurations of 32-bit and 64-bit host and guest operating systems running on multiprocessor host machines, versions 5.5 and later of Workstation support two-way virtual symmetric multiprocessing (SMP). This enables you to assign two virtual processors to a virtual machine. This is supported only for host machines with at least two logical processors. See [“Use Two-Way Virtual Symmetric Multiprocessing”](#) on page 348.

NOTE If the host is a uniprocessor machine, assigning two processors is not supported. A warning message appears. You can disregard this message and assign two processors to the virtual machine, but when you finish creating the virtual machine, you cannot power it on unless you move it to a host machine with at least two logical processors.

Open a Virtual Machine Created in ESX Server That Has More Than Two Processors

You can use Workstation 5.5 or higher, running on a multiprocessor host machine, to open a virtual machine created in VMware ESX Server that has one or more virtual

processors. However, in Workstation you cannot power on or resume a virtual machine that has more than two virtual processors assigned, even if more processors were assigned when the virtual machine was created in ESX Server.

You can see this setting in the virtual machine's summary view or by using the virtual machine settings editor.

To open a virtual machine created in ESX Server that has more than two processors

- 1 From the Workstation menu bar, choose **VM > Settings > Hardware > Processors**, and note that **Number of Processors** is set to **Other (x)**, where x is the number of processors originally assigned in ESX Server.

Workstation preserves this original configuration setting for the number of processors, even though two is the maximum number of processors supported.

- 2 Change this setting to two processors so that you can power on the virtual machine in Workstation.

After you commit a change to this setting, the original setting for number of processors is discarded, and no longer appears as an option in the virtual machine settings editor.

Move a Virtual Machine to a New Location or a New Host

Use the procedure in this section either to move the virtual machine to a different location on the same host or to move it to a new host. This section applies to virtual machines created with all these VMware products:

- Workstation 4.x, 5.x, 6.x
- GSX Server 3.x
- VMware Server 1.x
- ESX Server 2.x or 3.x
- VMware ACE 1.x, 2.x

For more information about virtual machine formats from older VMware products, see [“Legacy Virtual Disks”](#) on page 231.

To move a virtual machine to a new location or a new host

- 1 Make sure that all the virtual machine files are stored in the virtual machine directory.

For example, if you configured the working directory to be located in a different location on the host, move it into the virtual machine directory and use the virtual

machine settings editor (**VM > Settings > Options > General**) to point to this location.

If the virtual machine you want to move is a linked clone, see [“Moving Linked Clones”](#) on page 209.

- 2 Shut down the guest operating system and power off the virtual machine.
- 3 Copy all the files in the virtual machine directory to the new location.

To move the virtual machine's files to another host, if you don't have a network connection to the new host, use a shared network directory, burn the files onto a DVD, or use some other storage media that has enough disk space.

For more information about the files that you are moving, see [“Files That Make Up a Virtual Machine”](#) on page 100.

- 4 Start Workstation, choose **File > Open**, and browse to the virtual machine's configuration (.vmx) file in its new location.

For information about moving an ESX Server virtual machine with more than two processors, see [“Use a Virtual Machine That Originally Had More Than Two Virtual Processors”](#) on page 348.

- 5 (Optional) If you are moving the virtual machine to a different location on the same host, remove the virtual machine from the **Favorites** list and add it again using the new location.
- 6 When you are certain that the virtual machine in the new location works correctly, delete the virtual machine files from the old location, if desired.

If the virtual machine in the new location is not working correctly, examine the virtual machine in the original location to determine if you missed copying some files. Some files might reside outside of the virtual machine directory.

Use the virtual machine settings editor (**VM > Settings > Hardware**) to select devices and determine whether any associated files point to locations that cannot be accessed from the new virtual machine.

Workstation generates a different MAC address for the virtual Ethernet adapter when you move a virtual machine to a new host computer or to a different directory on the same host computer. A new MAC address is also generated when you rename a directory in the path to the virtual machine's configuration file. See [“Maintaining and Changing the MAC Address of a Virtual Machine”](#) on page 282.

Moving an Older Virtual Machine

If you created a virtual machine by using Workstation 2.x or 3.x, you must upgrade it to at least version 4. Workstation 6 does not support Workstation 2 or 3 virtual machines.

Moving Linked Clones

You can move a linked clone as you do an ordinary Workstation virtual machine. However, if you move a linked clone (or if you move its parent virtual machine), make sure the clone can access the parent virtual machine. Place the parent in shared directory or on a networked file server.

For example, if you put a linked clone on a laptop, and the parent remains on another machine, you can use the clone only when the laptop connects to the network or drive where the parent is stored. To use a cloned virtual machine on a disconnected laptop, you must use a full clone or you must move the parent virtual machine to the laptop.

You cannot power on a linked clone if Workstation cannot locate the original virtual machine.

Sharing Virtual Machines with Other Users

If you want other users to be able to access your virtual machines, consider the following points:

- Only one user can run a virtual machine at a time. Other users can also share a virtual machine by making a linked clone of it. A linked clone is a copy that uses the same virtual disks as the parent virtual machine it was copied from. See [“Cloning a Virtual Machine”](#) on page 201.
- On Windows hosts, relocate the virtual machine files to a directory that is accessible to all appropriate users. The default location for a Windows host is not typically accessible to other users:
 - On Windows XP: C:\Documents and Settings\<user_name>\My Documents\My Virtual Machines
 - On Windows Vista: C:\Users\<user_name>\Documents\Virtual Machines

When you configure the virtual machine in the New Virtual Machine wizard, you can specify a location for the virtual machine elsewhere on your system or on a network volume.

- On Linux hosts, set permissions for the virtual machine files appropriately.

Permissions settings are especially important for the configuration file (.vmx) and virtual disks (.vmdk). For example, if you want users to run a virtual machine but not be able to modify its configuration, do not make the configuration file writable.

Sharing Virtual Machines with VMware Player

VMware Player is a free application that opens and plays virtual machines created with other VMware products. On Windows hosts, Player also opens and plays Microsoft Virtual PC and Virtual Server virtual machines and Symantec LiveState Recovery and system images.

VMware Player is included with Workstation versions 5.5 and later. "Standalone" Player is also freely available for download at:

<http://www.vmware.com/products/player/>

VMware Player makes your VMware virtual machines accessible to colleagues, partners, customers, and clients who do not own other VMware products.

NOTE Use of VMware Player is subject to the VMware Player End User License terms, and no technical support is provided by VMware for VMware Player. For self-help resources, see the VMware Player FAQ at:

www.vmware.com/products/player/faqs.html

Also check the VMware Player Discussion Forum on the VMware VMTN Web site, at:

<http://communities.vmware.com/community/vmtn/desktop/player>

The forum is a site where VMTN members exchange information, questions, and comments regarding VMware products, services, and product support issues.

Start and Exit VMware Player

VMware Player is included in the Workstation distribution. When you install Workstation, the application file (vmpayer.exe on Windows or vmpayer on Linux), is stored with the rest of your Workstation program files.

To start and exit VMware Player

- 1 Open VMware Player, either from the graphical user interface (GUI) or from the command line:
 - From the GUI, on Windows, choose **VMware Player** from the **Start > Programs > VMware** menu.

In a Linux X session, choose **VMware Player** from the corresponding program menu, such as the **System Tools** menu.

- From the command line, open a command prompt, and enter one of the following commands:
 - On Windows, enter `<path>vmplayer.exe`
where `<path>` is the path on your system to the application file.
 - On Linux, enter `vmplayer &`

From the Welcome page, you can:

- Browse to a virtual machine file.
 - Open a recently used virtual machine.
 - Download a virtual appliance from the VMTN (VMware Technology Network) Web site.
- 2 Open a virtual machine.

For instructions on using and configuring VMware Player, see the online help provided in VMware Player. From the VMware Player menu bar, choose **VMware Player > Help**.

- 3 To exit VMware Player, do one of the following:
- Shut down the guest operating system in the virtual machine.
VMware Player closes after the guest operating system shuts down.
 - In VMware Player, choose **VMware Player > Exit** (Windows) or **Player > Quit** (Linux).

VMware Player either suspends or powers off the virtual machine, depending on the preference you set for exit behavior in **Player > Preferences**.

Setting Up Virtual Machines for Use with VMware Player

When you create a virtual machine that you intend to distribute to other users, configure the virtual machine for maximum compatibility with all expected host systems. Because the configuration options for VMware Player are limited, users are limited in their ability to make changes in a virtual machine so that it is compatible with their host systems.

Following are recommendations to help you configure virtual machines for maximum compatibility with VMware Player and with the widest range of host machines:

- Determine which virtual devices are actually required, and don't include any that are not needed or useful for the software you are distributing with the virtual machine and VMware Player. For example, generic SCSI devices are extremely unlikely to be appropriate.
- To connect a physical device to a virtual device, use the **Auto detect** options when configuring the virtual machine. The **Auto detect** options allow the virtual machine to adapt to the user's system, and they work whether the host operating system is Windows or Linux. Users who have no physical device receive a warning message.
- To connect a CD-ROM or floppy to an image file that you ship with the virtual machine, make sure the image file is in the same directory as the virtual machine. This way, a relative path, rather than an absolute path, is used.
- For both a physical CD-ROM and an image, provide two virtual CD-ROM devices in the virtual machine. VMware Player does not provide a way in the user interface to switch a single CD-ROM device between a physical CD-ROM and an image. This also means that if you want to ship multiple images, the user cannot switch between them.
- Choose a reasonable amount of memory to allocate to the virtual machine. If the user's host machine does not have enough physical memory to support the memory allocation, VMware Player cannot power on the virtual machine.
- Install VMware Tools in the virtual machine. VMware Tools significantly improves the user's experience working with the virtual machine.
- Choose a reasonable screen resolution for the guest. A user is likely to find it easier to increase the resolution manually than to deal with a display that exceeds the user's physical screen size.
- Some host operating systems do not support CD-ROMs in non-legacy mode. To ensure that CD-ROMs work properly in virtual machines that you intend to be distributed and played on VMware Player, configure CD-ROM devices in legacy mode. See ["Legacy Emulation for DVD and CD Drives"](#) on page 228.
- Select an appropriate setting in **VM > Settings > Options > Snapshots > When powering off**. Set this option to **Just power off** or **Revert to snapshot**. VMware Player does not allow taking snapshots.

The option **Revert to snapshot** is useful if you want to distribute a demo that resets itself to a clean state when powered off.

Using Disks and Disk Drives

12

This chapter provides information about how to configure virtual hard disk storage to best meet your needs. This chapter includes the following topics:

- [“Virtual Machine Disk Storage”](#) on page 213
- [“Virtual Disk Maintenance Tasks”](#) on page 217
- [“Adding Virtual and Physical Disks to a Virtual Machine”](#) on page 219
- [“Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine”](#) on page 227
- [“Using VMware Virtual Disk Manager”](#) on page 231
- [“Using Dual-Boot Computers with Virtual Machines”](#) on page 231
- [“Legacy Virtual Disks”](#) on page 231

To map an existing virtual disk drive to a Windows host machine, rather than adding it to a virtual machine, see [“Using a Mapped Drive for Windows Only”](#) on page 184.

Virtual Machine Disk Storage

Like a physical computer, a VMware Workstation virtual machine stores its operating system, programs, and data files on one or more hard disks. Unlike a physical computer, Workstation provides ways to undo changes to the virtual machine’s hard disk.

The New Virtual Machine wizard creates a virtual machine with one disk drive. Use the virtual machine settings editor (choose **VM > Settings**) to add more disk drives to your virtual machine, to remove disk drives from your virtual machine, and to change certain settings for the existing disk drives.

This section describes the choices you can make in setting up hard disk storage for a virtual machine.

Benefits of Using Virtual Disks

In most cases, it is best to configure virtual machines to use virtual hard disks rather than physical hard disks. A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. The files can be on the host machine or on a remote computer. When you configure a virtual machine with a virtual disk, you can install a new operating system onto the virtual disk without repartitioning a physical disk or rebooting the host.

Portability

A key advantage of virtual disks is their portability. Because the virtual disks are stored as files on the host machine or a remote computer, you can move them easily to a new location on the same computer or to a different computer. You can also use Workstation on a Windows host to create virtual disks, move them to a Linux computer, and use them with Workstation for Linux, and the reverse. See [“Moving a Virtual Machine”](#) on page 205.

Disk Size and Files

Virtual disks can be as large as 950GB (IDE or SCSI). Depending on the size of the virtual disk and the host operating system, Workstation creates one or more files to hold each virtual disk. These files include information such as the operating system, program files, and data files. The virtual disk files have a .vmdk extension.

By default, the actual files that the virtual disk uses start small and grow to their maximum size as needed. The main advantage of this approach is the smaller file size. Smaller files require less storage space and are easier to move to a new location. However, it takes longer to write data to a disk configured in this way.

You can also configure virtual disks so that all of the disk space is allocated when the virtual disk is created. This approach provides enhanced performance and is useful if you are running performance-sensitive applications in the virtual machine.

Regardless of whether you allocate all disk space in advance, you can configure the virtual disk to use a set of files limited to 2GB per file. Use this option if you plan to move the virtual disk to a file system that does not support files larger than 2GB.

Lock Files

A running virtual machine creates lock files to prevent consistency problems on virtual disks. Without locks, multiple virtual machines might read and write to the disk, causing data corruption.

Lock files are created in subdirectories with a `.lck` suffix. The locking subdirectories reside in the same directory as the virtual machine's `.vmdk` files. A locking subdirectory and lock file are created for `.vmdk` files, `.vmx` files, and `.vmem` files.

As of the Workstation 6 release, a unified locking method is used on all host operating systems, so files shared between them are fully protected. For example, if one user on a Linux host tries to power on a virtual machine that is already powered on by another user with a Windows host, the lock files prevent the second user from powering on the virtual machine.

When a virtual machine powers off, it removes the locking subdirectories and their lock files. If it cannot remove these locking controls, one or more stale lock files might remain. For example, if the host machine fails before the virtual machine removes its locking controls, stale lock files remain.

When the virtual machine restarts, it scans any locking subdirectories for stale lock files and, when possible, removes them. A lock file is considered stale if both of the following conditions are true:

- The lock file was created on the same host that is now running the virtual machine.
- The process that created the lock is no longer running.

If either of these conditions is not true, a dialog box warns you that the virtual machine cannot be powered on. You can delete the locking directories and their lock files manually.

Locks also protect physical disk partitions. However, the host operating system is not aware of this locking convention and thus does not respect it. For this reason, VMware recommends that the physical disk for a virtual machine not be installed on the same physical disk as the host operating system.

IDE and SCSI Disk Types

Virtual disks can be set up as IDE disks for any guest operating system. They can be set up as SCSI disks for any guest operating system with a driver for the LSI Logic or BusLogic SCSI adapter available in a Workstation virtual machine. You determine which SCSI adapter to use at the time you create the virtual machine.

NOTE To use SCSI disks in a 32-bit Windows XP virtual machine, download a special SCSI driver from the Downloads page of the VMware Web site. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP.

A virtual disk of either type can be stored on either type of physical hard disk. That is, the files that make up an IDE or SCSI virtual disk can be stored on either an IDE hard

disk or a SCSI hard disk. They can also be stored on other types of fast-access storage media.

Physical Disks

In some circumstances, you might need to give your virtual machine direct access to a physical hard drive on your host computer. A physical disk directly accesses an existing local disk or partition. You can use physical disks if you want Workstation to run one or more guest operating systems from existing disk partitions.



CAUTION Do not attempt physical disk configurations unless you are an expert user.

Although virtual disks are limited to 950GB, physical disks can be set up on both IDE and SCSI devices of up to 2TB capacity. Booting from an operating system already set up on an existing SCSI disk or partition is currently not supported.

Also, on Windows Vista hosts, you cannot use the system partition or the physical disk that contains it in a virtual machine.



CAUTION Running an operating system natively on the host computer and switching to running it inside a virtual machine is like pulling the hard drive out of one computer and installing it in a second computer with a different motherboard and hardware. The steps you take depend on the operating system you want to use inside the virtual machine. See the VMware technical note *Dual-Boot Computers and Virtual Machines*.

You can also create a new virtual machine that uses a physical disk. See [“Using Physical Disks in a Virtual Machine”](#) on page 221. In most cases, however, it is better to use a virtual disk. If you use a physical disk, the .vmdk file stores information about the physical disk or partition that the virtual machine uses.

After you configure a virtual machine to use one or more partitions on a physical disk, do not modify the partition tables by running `fdisk` or a similar utility in the guest operating system.

If you use `fdisk` or a similar utility on the host operating system to modify the partition table of the physical disk, you must re-create the virtual machine's physical disk. All files that were on the physical disk are lost when you modify the partition table.



CAUTION Do not use a physical disk to share files between host and guest operating systems. It is not safe to make the same partition visible to both host and guest. You can cause data corruption if you do this. To share files between host and guest operating systems, use shared folders. See [“Set Up Shared Folders”](#) on page 178.

Virtual Disk Maintenance Tasks

Defragmenting virtual disks can improve performance. Shrinking virtual disks reclaims any unused space.

Defragment Virtual Disks

Like physical disk drives, virtual disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual disk so that programs run faster and files open more quickly.

Before you begin, make sure you have adequate free working space on the host computer. If your virtual disk is contained in a single file, for example, you need free space equal to the size of the virtual disk file. Other virtual disk configurations require less free space.

Defragmenting does not reclaim unused space on a virtual disk. To reclaim unused space, shrink the disk. See [“Shrink a Virtual Disk”](#) on page 218.

To defragment a virtual disk

- 1 Run a disk defragmentation utility inside the guest operating system.
 For example, in a virtual machine with a Windows XP guest operating system, use the Windows XP Disk Defragmenter tool from within the virtual machine.
 Defragmenting disks can take considerable time.
- 2 If the virtual disk is “growable” rather than preallocated, defragment it by using the Workstation defragmentation tool:
 - a Select the virtual machine.
 - b Make sure the virtual machine is powered off.
 - c Choose **VM > Settings**.
 - d On the **Hardware** tab, select **Hard Disk**, and do one of the following:
 - On Linux hosts, click **Defragment**.
 - On Windows hosts, click **Utilities** and choose **Defragment**.
 - e When the process is finished, click **OK**.
- 3 Run a disk defragmentation utility on the host computer.
 Defragmenting disks can take considerable time.

Shrink a Virtual Disk

Shrinking a virtual disk reclaims unused space in the virtual disk. If a disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive.

Before you perform the procedure in this topic, make sure the following prerequisites are met:

- VMware Tools is installed in the guest operating system.
- The host has free disk space equal to the size of the virtual disk you plan to shrink.
- The disk space is not preallocated for the virtual hard disk. Use the virtual machine settings editor to view the disk information for this virtual hard disk. If the disk space was preallocated, you cannot shrink the disk.
- The virtual machine has no snapshots. If it has a snapshot, a **Snapshot** line appears in its summary view.

To delete a snapshot, choose **VM > Snapshot > Snapshot Manager**. Select the snapshot and click the **Delete** button (on Windows) or icon (on the snapshot toolbar on Linux).

- The virtual machine is not a linked clone or the parent of a linked clone. If the virtual machine is a linked clone, a **Clone of** line appears on its summary tab. If it is the parent of a linked clone, a **Snapshot** line appears on its summary tab.
- If the virtual hard disk is an independent disk, it is in persistent mode.

To change the mode, see [“Exclude a Virtual Disk from Snapshots”](#) on page 192 for a discussion of independent disks.

To shrink a virtual disk

- 1 Launch the VMware Tools control panel:
 - For a Windows guest, double-click the **VMware Tools** icon in the notification area of the taskbar.

If the icon is not available, choose **Start > Settings > Control Panel**, and double-click **VMware Tools**.
 - For a Linux, Solaris, or FreeBSD guest, open a terminal window, become root, and run `vmware-toolbox`.

If you shrink disks as a nonroot user, you cannot wipe the parts of the virtual disk that require root-level permissions.
- 2 In the VMware Tools control panel, click the **Shrink** tab.

If the virtual machine does not allow shrinking, the **Shrink** tab shows the reason.

- 3 Select virtual disks to shrink and click **Prepare to Shrink**.

If you deselect some partitions, the whole disk still shrinks. However, those partitions are not wiped for shrinking, and the shrink process does not reduce the size of the virtual disk as much as it would with all partitions selected.

VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. During this phase, you can still interact with the virtual machine.

VMware Tools finishes wiping the selected disk partitions, a prompt to shrink disks appears.

- 4 Click **Yes**.

Shrinking disks can take considerable time.

- 5 Click **OK**.

Adding Virtual and Physical Disks to a Virtual Machine

This section provides instructions for creating virtual disks, removing disks, adding existing disks to virtual machines, and using physical disks in a virtual machine.

You can connect other SCSI devices to a virtual machine by using the generic SCSI driver for the host operating system. See [“Add a Generic SCSI Device to a Virtual Machine”](#) on page 345.

Create a Virtual Disk and Add It to a Virtual Machine

Virtual disks are stored as files on the host computer or on a network file server. A virtual IDE drive or a virtual SCSI drive can be stored on an IDE drive or on a SCSI drive.

NOTE If you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

To add a new virtual disk to a virtual machine

- 1 Select the virtual machine.
Make sure the virtual machine is powered off.
- 2 Choose **VM > Settings**.
- 3 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.

- 4 On the Hardware Type page, select **Hard Disk** and click **Next**.
- 5 On the Select a Disk page, select **Create a new virtual disk** and click **Next**.
- 6 On the Select a Disk Type page, choose **IDE** disk or **SCSI**.

For information about SCSI disk requirements, see [“IDE and SCSI Disk Types”](#) on page 215.

Workstation 6 virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

- 7 (Optional) To exclude disks from snapshots, in the **Mode** section, select **Independent** for the mode and choose one of the following options:
 - **Persistent** – Changes are immediately and permanently written to the disk.
 - **Nonpersistent** – Changes to the disk are discarded when you power off or revert to a snapshot.

See [“Information Captured by Snapshots”](#) on page 191.

- 8 On the Specify Disk Capacity page, set the capacity for the new virtual disk.
You can set a size between 0.1GB and 950GB for a virtual disk. See [“Disk Size and Files”](#) on page 214.
- 9 On the Specify Disk File page, accept the default filename and location or browse to and select a different location and click **Finish**.
The wizard creates the new virtual disk. It appears to your guest operating system as a new, blank hard disk.
- 10 In the virtual machine settings editor, click **OK**.
- 11 Use the guest operating system tools to partition and format the new drive for use.

Add an Existing Virtual Disk to a Virtual Machine

You can reconnect an existing virtual disk that was removed from a virtual machine.

Workstation 6 virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

To add an existing virtual disk to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.

- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
- 5 On the Hardware Type page, select **Hard Disk** and click **Next**.
- 6 On the Select a Disk page, select **Use an existing virtual disk** and click **Next**.
- 7 On the Select an Existing Disk page, specify the path name and filename for the existing disk file and click **Finish**.
- 8 In the virtual machine settings editor, click **OK**.

Remove a Virtual Disk from a Virtual Machine

Removing a virtual disk disconnects it from a virtual machine. Removing the virtual disk does not delete files from the host file system.

Use the procedure in this topic to map or mount the disk to a host machine. After you remove the disk from the virtual machine, you can map or mount it to a host and copy data from the guest to the host without powering on the virtual machine or starting Workstation.

To remove a virtual disk from a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, select a virtual disk and click **Remove**.

The virtual disk is disconnected from virtual machine.

After you remove the disk from the virtual machine, you can do either of the following:

- Map the disk to the host. See [“Using a Mapped Drive for Windows Only”](#) on page 184.
- Add the disk to another virtual machine. See [“Add an Existing Virtual Disk to a Virtual Machine”](#) on page 220.

Using Physical Disks in a Virtual Machine

You can install a guest operating system directly on an unused physical disk or unused partition. However, an operating system installed in this setting probably cannot boot outside of the virtual machine, even though the data is available to the host. For

information about using an operating system that can also boot outside of the virtual machine, see the VMware's *Dual-Boot Computers and Virtual Machines* technical note.

Physical disks are an advanced feature. Do not configure them unless you are an expert user. To use a physical disk in a virtual machine, you can add the physical disk to an existing virtual machine, or create a virtual machine and specify which physical disk the virtual machine uses.

Prerequisites for Using a Physical Disk

Before you run the New Virtual Machine wizard or use the virtual machine settings editor to add a physical (raw) disk, perform the following tasks:

- Because the virtual machine and guest operating system access a physical disk partition while the host continues to run its operating system, verify that the partition is not mounted by the host or in use by another virtual machine.

Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted on the host operating system.
- Check the guest operating system documentation regarding the type of partition on which the operating system can be installed.
 - On Windows Vista hosts, you cannot use the system partition or the physical disk that contains it in a virtual machine.
 - DOS, Windows 95, and Windows 98 operating systems must be installed on the first primary partition.
 - Other operating systems, such as Linux, can be installed on a primary or an extended partition on any part of the drive.
- Make sure the physical partition or disk does not have data you need in the future. If it does, back up the data.
- On Windows hosts:
 - If you use a Windows host's IDE disk in a physical disk configuration, make sure it is not configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.
 - If your host is running Windows 2000, Windows XP, or Windows Server 2003, do not use a dynamic disk as a physical disk in a virtual machine. Use the disk management tool to check the disk type and change a dynamic disk to a basic disk, which destroys all data. See ["Change a Windows Disk Type from Dynamic to Basic"](#) on page 223.

- Make sure the partition you want to use is unmapped. See [“Unmap a Partition That Is Mapped to a Windows NT Host”](#) on page 223.
- On Linux hosts, set the device group membership or device ownership appropriately. See [“Set Permissions on Linux Hosts”](#) on page 224.

After you determine that the physical disk meets these prerequisites, use either of the following strategies to use the physical disk in a virtual machine:

- [“Create a Virtual Machine That Uses a Physical Disk”](#) on page 225
- [“Add a Physical Disk to an Existing Virtual Machine”](#) on page 226

Change a Windows Disk Type from Dynamic to Basic

To use a hard disk in a virtual machine whose host is running Windows 2000, Windows XP, or Windows Server 2003, the virtual machine must use a basic disk.

To change a Windows disk type from dynamic to basic

- 1 On the host, choose **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**.

The disk management tool opens.

- 2 Delete all logical volumes on the disk.

This action destroys all data on the disk.

- 3 Right-click the disk icon and select **Revert to Basic Disk**.

- 4 Partition the disk.

Unmap a Partition That Is Mapped to a Windows NT Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows NT host

- 1 Choose **Start > Programs > Administrative Tools**.

The Disk Administrator appears.

- 2 Highlight the partition on which you plan to install the guest operating system, and choose **Tools > Assign Drive Letter**.

- 3 Choose **Do not assign a drive letter for the partition** and click **OK**.

The unmapping happens immediately.

Unmap a Partition That Is Mapped to a Windows Server 2003, Windows XP, or Windows 2000 Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows Server 2003, Windows XP, or Windows 2000 host

- 1 Choose **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**.
- 2 Select a partition and choose **Action > All Tasks > Change Drive Letter and Paths**.
- 3 Click **Remove**.

Unmap a Partition That Is Mapped to a Windows Vista Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows Vista host

- 1 Choose **Start > Control Panel (Classic View) > Administrative Tools > Computer Management > Storage > Disk Management**.
- 2 Right-click a partition and choose **Change Drive Letter and Paths**.
- 3 Click **Remove**.

Set Permissions on Linux Hosts

If permissions are set correctly, the physical disk configuration files in Workstation guard access. This reliability provides boot managers access to configuration files and other files they might need to boot operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that might be on another drive.

To set permissions on Linux hosts

- 1 Make sure the master physical disk device or devices are readable and writable by the user who runs Workstation.
 - Physical devices, such as `/dev/hda` (IDE physical disk) and `/dev/sdb` (SCSI physical disk), belong to group-id `disk` on most distributions. If this is the case, you can add VMware Workstation users to the `disk` group.
 - Another option is to change the owner of the device. Consider all the security issues involved in this option.

- 2 Grant VMware Workstation users access to all `/dev/hd[abcd]` physical devices that contain operating systems or boot managers.

Create a Virtual Machine That Uses a Physical Disk

Use the New Virtual Machine wizard to create a new virtual machine that uses a physical disk rather than adding a physical disk to an existing virtual machine.

Before you begin, complete the tasks described in [“Prerequisites for Using a Physical Disk”](#) on page 222.

To create a virtual machine that uses a physical disk

- 1 Use the New Virtual Machine wizard to create a virtual machine that uses a physical disk.

Follow the instructions in [“Create a Virtual Machine by Using the Custom Setup”](#) on page 94. On the Select a Disk page of the wizard, select **Use a physical disk**, and choose to use individual partitions or the entire disk.

If you use individual partitions, only the partitions you select are accessible to the virtual machine. The other partitions might be visible to the guest operating system, but you cannot mount, access, or format them.

- 2 (Optional) To specify a device node for the virtual disk or exclude disks from snapshots, do the following:
 - a Select the virtual machine and choose **VM > Settings**.
 - b On the **Hardware** tab, select the physical disk and click **Advanced**.
 - c To change the device node, select from the **Virtual device node** list.
 - d To exclude disks from snapshots, select **Independent** for the mode and choose one of the following options:
 - **Persistent** – Changes are immediately and permanently written to the disk.
 - **Nonpersistent** – Changes to the disk are discarded when you power off or revert to a snapshot.

See [“Information Captured by Snapshots”](#) on page 191.

- 3 Install the guest operating system on the physical disk.

For more information about supported operating systems, see the *VMware Guest Operating System Installation Guide*. This guide is available from the Workstation **Help** menu.

Add a Physical Disk to an Existing Virtual Machine

Use the virtual machine settings editor, rather than the New Virtual Machine wizard, to add a physical disk to an existing virtual machine.

Before you begin, complete the tasks described in [“Prerequisites for Using a Physical Disk”](#) on page 222.

To add a physical disk to an existing virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add**.
- 5 On the Hardware Type page, select **Hard Disk** and click **Next**.
- 6 On the Select a Disk page, select **Use a physical disk** and click **Next**.
- 7 If a warning appears, click **OK**.
- 8 On the Select a Physical Disk page, do the following:
 - a Choose the physical hard disk to use from the drop-down list.
Workstation supports physical disks up to 2TB.
 - b Select whether you want to use the entire disk or only individual partitions on the disk and click **Next**.
- 9 If you selected **Use individual partitions**, select the partitions you want to use in the virtual machine and click **Next**.
The virtual machine can access only the partitions you select. The guest operating system might be able to detect other partitions, but you cannot mount, access, or format them.
- 10 On the Specify Disk File page, accept the default filename and location or browse to a different location.
- 11 (Optional) To specify a device node for the virtual disk or exclude disks from snapshots, do the following:
 - a On the Specify Disk File page, click **Advanced**.
 - b To change the device node, select from the **Virtual device node** list.
 - c To exclude disks from snapshots, select **Independent** for the mode and choose one of the following options:

- **Persistent** – Changes are immediately and permanently written to the disk.
- **Nonpersistent** – Changes to the disk are discarded when you power off or revert to a snapshot.

See [“Information Captured by Snapshots”](#) on page 191.

12 Click **Finish**.

The wizard configures the new physical disk.

13 Use the guest operating system’s tools to format any partitions on the physical disk that are not formatted for your guest operating system.



CAUTION After you add a virtual machine disk by using one or more partitions on a physical disk, never modify the partition tables by running `fdisk` or a similar utility in the guest operating system. If you do so, you must re-create the virtual machine’s physical disk.

Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine

Workstation 6 virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

A virtual machine can read data from a DVD disc. Workstation does not support playing DVD movies in a virtual machine. You might be able to play a movie if you use a DVD player application that does not require video overlay support in the video card.

This section describes how to configure a virtual machine to use a host DVD drive, CD-ROM drive, or floppy disk drive. It also tells how to connect virtual CD-ROM or DVD drives and floppy drives to image files.

Add DVD or CD Drives to a Virtual Machine

You can add one or more DVD or CD drives to your virtual machine. You can connect the virtual DVD or CD drive to a physical drive on the host machine or to an ISO image file.

You can configure the virtual DVD or CD drive as either IDE or SCSI regardless of the type of physical drive you connect it to. For example, if your host computer has an IDE CD drive, you can set up the virtual machine drive as either SCSI or IDE and connect it to the host drive. The same is true if the physical drive on the host is a SCSI drive.

To add a DVD or CD drive to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add**.
- 5 On the Hardware Type page, select **DVD/CD-ROM Drive** and click **Next**.
- 6 Make a selection on the Select a Drive Connection page and click **Next**.
- 7 (Optional) If you select **Use physical drive**:
 - a Choose a drive from the drop-down list or choose **Auto detect**.
 - b To not connect the CD drive when the virtual machine starts, deselect **Connect at power on**.
 - c To specify which device node the drive uses in the virtual machine, click **Advanced**.

Select **Legacy emulation** only if you experienced problems using normal mode. See [“Legacy Emulation for DVD and CD Drives”](#) on page 228.
 - d Click **Finish**.
- 8 (Optional) If you select **Use ISO image**:
 - a Enter the path and filename for the image file or browse to the file.
 - b To not connect the CD drive when the virtual machine starts, deselect **Connect at power on**.
 - c To specify which device node the drive uses in the virtual machine, click **Advanced**.
 - d Click **Finish**.

The drive is set up initially so that it appears as an IDE drive to the guest operating system.

- 9 (Optional) To make the drive appear to the guest operating system as a SCSI drive, click the entry for that drive in the virtual machine settings editor and edit the settings in the panel on the right.

Legacy Emulation for DVD and CD Drives

In normal mode (that is, not legacy emulation mode), the guest operating system communicates directly with the CD or DVD drive. This direct communication enables

you to read multisession CDs, perform digital audio extraction, view videos, and use CD and DVD writers to burn discs.

Legacy emulation mode enables you to read only from data discs in the DVD or CD drive. It does not provide the other capabilities of normal mode. Use legacy emulation mode to work around direct communication problems between a guest operating system and a DVD or CD drive.

Use the virtual machine settings editor (**VM > Settings**) to set the **Legacy emulation** option for DVD and CD drives attached to the virtual machine:

- On Windows hosts, this option is deselected by default.
- On Linux hosts with IDE drives, the default setting depends on whether the `ide-scsi` module is loaded in your kernel. The `ide-scsi` module must be loaded, or you must be using a physical SCSI drive to connect directly to the DVD or CD drive.

If you run more than one virtual machine at a time, and if their CD drives are in legacy emulation mode, start the virtual machines with their CD drives disconnected. This ensures that multiple virtual machines are not connected to the CD drive at the same time.

Add Floppy Drives to a Virtual Machine

You can add up to two floppy drives to a virtual machine. A virtual floppy drive can connect to a physical floppy drive on the host computer, to an existing floppy image file, or to a blank floppy image file.

To add a floppy drive to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add**.
- 5 On the Hardware Type page, select **Floppy Drive** and click **Next**.
- 6 Follow the instructions to complete the wizard.

- 7 (Optional) If you are adding a second floppy drive to the virtual machine, enable this second floppy drive in the virtual machine BIOS, as follows:
 - a Boot the virtual machine, and as it boots, click in the virtual machine window and press F2 to enter the BIOS setup utility.
 - b On the main screen, choose **Legacy Diskette B:** and use the plus (+) and minus (-) keys on the numerical keypad to select the type of floppy drive to use.
 - c Press F10 to save the settings.

Connect a CD-ROM, DVD, or Floppy Drive to an Image File

You can connect an existing virtual CD-ROM, DVD, or floppy drive to an image file (ISO file) rather than the physical drive on the host. An ISO image file resembles a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer.

In some host configurations, the virtual machine cannot boot from the installation CD-ROM. To avoid that problem, create an ISO image file from the installation CD-ROM.

To connect a CD-ROM or floppy drive to an image file

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, select a DVD, CD-ROM, or floppy drive.
- 5 Do one of the following:
 - For a DVD or CD-ROM drive, select **Use ISO Image** and specify the path name and filename.
 - For a floppy drive:
 - If the file already exists, select **Use floppy Image** and specify the path name and filename.
 - To create an image file, click **Create**, browse to the directory where you plan to store the floppy image file, supply a filename, and click **Save** (on Windows hosts) or **Open** (on Linux hosts).
- 6 (Optional) To make the file read only, select the **Read Only** check box.
- 7 Click **OK**.

Using VMware Virtual Disk Manager

VMware Virtual Disk Manager is a Workstation utility that allows you to create, manage, and modify virtual disk files from the command line or in scripts.

You can enlarge a virtual disk so that its maximum capacity is larger than it was when you created it. This is useful if you need more disk space in a given virtual machine, but do not want to add another virtual disk or use ghosting software to transfer the data on a virtual disk to a larger virtual disk. You cannot do this with physical hard drives.

You can also change disk types. When you create a virtual machine, you specify how disk space is allocated, as follows:

- All space for the virtual disk is allocated in advance. This corresponds to the preallocated disk type for Virtual Disk Manager.
- Space allocated for the virtual disk begins small and grows as needed. This corresponds to the growable disk type for Virtual Disk Manager.

If you allocate all the disk space for a virtual disk but later need to reclaim some hard disk space on the host, you can convert the preallocated virtual disk into a growable disk. The new virtual disk is still large enough to contain all the data in the original virtual disk.

You can also change whether the virtual disk is stored in a single file or split into 2GB files.

These features and the ability to use scripting to automate management of virtual disks were added to Workstation in version 5.0. See the VMware technical note about using Virtual Disk Manager.

Using Dual-Boot Computers with Virtual Machines

Some users install Workstation on a dual-boot or multiple-boot computer so that they can run one or more of the existing operating systems in a virtual machine. For more information about using dual-boot computers with Workstation, see the VMware *Dual-Boot Computers and Virtual Machines* technical note.

Legacy Virtual Disks

You have several options for using Workstation 6 in a mixed environment with virtual machines that were created with earlier versions of Workstation or created with other VMware products.

Following is a brief summary of feature compatibility between various virtual hardware versions of Workstation:

- A Workstation 6.x virtual machine supports all Workstation 6.x features but is compatible with a limited number of other VMware products.
- A Workstation 5 virtual machine is compatible with VMware Server 1.x, ESX Server 3.x, and VMware Player 1.x.

Workstation versions 5.5 and later support 64-bit guest operating systems.

- A Workstation 4 virtual machine is compatible with VMware GSX Server 3.x, ESX Server 2.x, and ACE 1.0.

For more compatibility information, see the *VMware Virtual Machine Mobility Planning Guide*.

You can use Workstation 6 to power on virtual machines created with any of the product versions in this list. However, many new features of Workstation are not available in older virtual machines. To upgrade your virtual machines to Workstation 6, see [“Change the Version of the Virtual Machine”](#) on page 57.

If you decide not to upgrade a virtual machine, VMware recommends that you upgrade VMware Tools to the latest version. See [“VMware Tools Update Process”](#) on page 117. Do not remove the older version of VMware Tools before installing the new version.

You can also use Workstation 6 to create a version 4 or 5 virtual machines. See [“Create a Virtual Machine by Using the Custom Setup”](#) on page 94.

NOTE If you have Workstation 2 or 3 virtual machines that you want to use with Workstation 6, upgrade the virtual machines to at least Workstation version 4 before you attempt to power them on with Workstation 6.

Recording and Replaying Virtual Machine Activity

13

The record/replay feature you to record all of a Workstation 5, 6, or 6.5 virtual machine's activity over a period of time. This chapter includes the following topics:

- [“Uses of the Record/Replay Feature”](#) on page 233
- [“Physical and Virtual Hardware Requirements”](#) on page 234
- [“Enabling Record/Replay for a Virtual Machine”](#) on page 235
- [“Making a Recording”](#) on page 238
- [“Replaying a Recording”](#) on page 239
- [“Creating an Execution Trace File of a Recording”](#) on page 240
- [“Maintenance Tasks for Using Recordings”](#) on page 241

Uses of the Record/Replay Feature

Unlike Workstation's movie-capture feature, the record/replay feature records all the processor instructions of the virtual machine throughout the time of the recording. This feature helps software developers and QA engineers to record a bug and attach a debugger while replaying the recording.



CAUTION Features with experimental support are not enabled on production systems. Enabling the record/replay feature might cause the host to crash, causing you to lose data.

After you enable the record/replay feature for a virtual machine, start recording by clicking the **Record** button and click the **Stop** button to end the recording. You can make multiple recordings and use the snapshot manager to name, delete, and play them. While you are making a recording you can take snapshots of events and replay

them. You can also make an execution trace file of a recording to record events that occur during the recording.

Playing a recording is in some respects similar to going to a snapshot. When you play a recording, you discard the current state of the virtual machine and go to the recording. At any time when the recording is playing, you can click the **Go Live** button and resume interacting with the guest operating system at the state the virtual machine is in when you click **Go Live**.

NOTE Recordings are not interchangeable between different versions of Workstation. The recordings made with this release will not work with Workstation 6 and upcoming 6.5 versions.

The sections that follow provide details about how to enable this feature and use it.

Physical and Virtual Hardware Requirements

Following is a list of requirements for and limitations of this feature:

- Host CPUs – For optimum performance, use a computer with an Intel P4 processor or equivalent when using this feature.

If you use the record/replay feature on a host computer that does not have an Intel P4 processor, when you enable the record/replay feature and power on the virtual machine, a message appears, informing you that recording is not supported on your processor. Supported processors include Pentium 4, Intel Core 2, Greyhound, Next-Generation Intel Microarchitecture - Nehalem, and Penryn/Harpertown. Other processors might operate more slowly during recording and replaying.

- Virtual machine version – Only Workstation 5, 6, and 6.5 virtual machines can be recorded.
- Supported operating systems – You can use the record/replay feature only on 32-bit versions of the following guest operating systems:
 - Windows 2000, XP, 2003, Vista
 - Red Hat Enterprise Linux 3 and 4
 - SUSE Linux 9.3 and 10.x
- Unsupported operating systems – You cannot use the record/replay feature on 64-bit versions of the guest operating system.

If you attempt to enable the record/replay feature on an unsupported operating system, the virtual machine will not power on until you disable record/replay. In addition, SMP and paravirtualization on VMI are not supported.

- **Unsupported virtual devices** – Before you enable the record/replay feature, use the virtual machine settings editor to remove the sound adapter from the virtual machine and disconnect the Floppy device.

In addition, avoid connecting the virtual machine to a network or disconnecting it during a recording session.

- **Disk space** – How much disk space a recording uses depends on the type of activity that occurs on the virtual machine and the duration of the recording session. By default a screenshot is created every five seconds. Therefore, assume that you will need several megabytes of disk space for one minute of recording.

NOTE If you have a number of high-resolution virtual machines open on your screen it will consume more disk space.

- **Disk mode** – You cannot use the record/replay feature if the virtual machine's virtual hard disk is set to independent mode. This is because recording virtual machine activity requires writing data about the disk to a "continual snapshot." Use the virtual machine settings editor to change the disk mode, choose **VM > Settings > Hardware > Hard Disk > Advanced**.

Enabling Record/Replay for a Virtual Machine

Make sure that the virtual machine meets the requirements listed in ["Physical and Virtual Hardware Requirements"](#) on page 234.

NOTE When you enable the record/replay feature, the debugging mode automatically gets set to **Full**. If you later disable record/replay, you need to manually set debugging mode back to **Normal**. See ["Set the Debugging Mode"](#) on page 242.

To enable record/replay for a virtual machine

- 1 Make sure the virtual machine is powered off.
- 2 Select the virtual machine and choose **VM > Settings**.
The virtual machine settings editor appears.
- 3 Click the **Options** tab, and select **Snapshot/Replay**.
- 4 On the **Snapshot/Replay** settings panel, select the **Enable replay** check box.
- 5 (Optional) As a safety precaution, use the **When Recording** controls to limit how much disk space the recording can use.
 - Setting the Max disk space to **Unlimited** uses much more disk space than setting it to **500MB**.

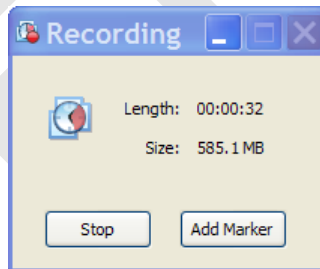
- Selecting the **Save the last** sets the duration of the time you want to save the recording. Setting the Marker frequency to **High (every 1 hour)** uses much more disk space than setting it to **Low (every 6 hours)**.
- 6 (Optional) Select the **Enable VAssert** check box if you plan to use VMware VAssert to debug applications.

VAssert enables developers and support engineers to take advantage of traditional assert and logging capabilities to debug errors in replay logs. The asserts appear only during replay of a recording.
- 7 Click **OK**.

Record Control Dialog Box Features

On Windows, a record control dialog box appears when you click the **Record** button in the toolbar. On Linux, the record options are located in the toolbar.

Figure 13-1. Windows Record Control Dialog Box



- **Stop** – Stops the recording that is in progress.
- **Add Marker** – Takes a replay-specific snapshot at the current location within the recording. You can use this marker during replay to skip ahead in a recording.
- **Minimize** – On Windows, the (-) button minimizes the record control dialog box to the lower-left side of the status bar. The minimized control allows you to work on your virtual machine and use the controls in the status bar to either stop a recording or add a marker.

NOTE Keep in mind that you cannot close the record control dialog box.

Replay Control Dialog Box Features

The replay control dialog box appears when you replay a recording.

Figure 13-2. Windows Replay Control Dialog Box

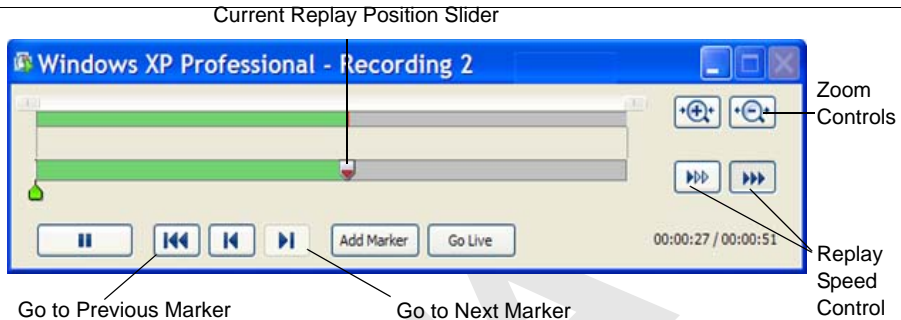
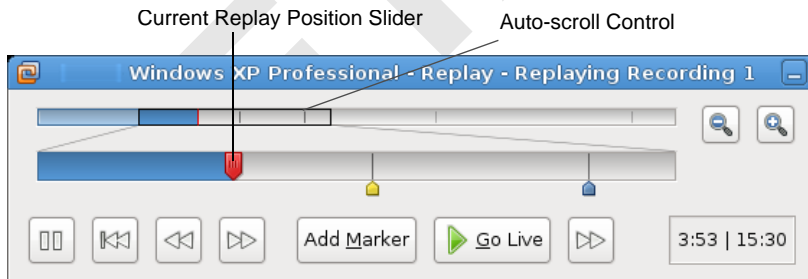


Figure 13-3. Linux Replay Control Dialog Box



The replay control dialog box contains the following buttons:

- **Play/Pause** – The button is labeled **Play** if you want to play the last recording you made for the selected virtual machine. If the virtual machine is powered off, it is resumed, as if it had been suspended. It is labeled **Pause** if you want to suspend the replay and click the button again to resume replay.
- **Go Live** – Stops the replay that is in progress and reverts to the current state of the virtual machine.
- **Add Marker** – Takes a replay-specific snapshot at the current location within the recording. You can use this marker during replay to skip ahead in a recording.
- **Go to Previous Marker** – Plays the previous marker.

- **Go to Next Marker** – Plays the next marker.
- **Current Replay Position Slider** – Allows to preview a replay. You can drag and drop the **Current Replay Position Slider** to the nearest previous snapshot and start replaying. On Linux, the auto-scroll function of the zoomed in portion is enabled. The **Current Replay Position Slider** is a red arrow located in the progress timeline.
- **Zoom Control** – Controls the zoom in and out function during replay.
- **Minimize** – On Windows, the (-) button minimizes the dialog box to the bottom left hand side of the status bar. The minimized control allows you to view your recording in the virtual machine and use the controls in the status bar. The progress indicator in the status bar shows the timeline of the recording.

NOTE Keep in mind that you cannot close the replay control dialog box.

- **Replay Speed Control** – Controls the replay speed of a recording. Click the right button to increase the replay speed to the maximum. Click the left button to decrease the replay speed to normal.

NOTE The speed of a playback depends on the host activity and workload of the guest.

Making a Recording

While making a recording you cannot pause or reverse it.



CAUTION While a recording is in progress, avoid exiting Workstation and allowing the virtual machine to run in the background. Doing so might cause the virtual machine to crash. Always stop recording before sending a virtual machine to run in the background.

Before you begin, verify the screen resolution settings. The resolution cannot be changed during replay. If you change from windowed mode to full-screen mode during replay, the auto-fit feature does not work.

To make a recording

- 1 Power on the virtual machine.
- 2 To begin recording, click the **Record** button in the toolbar, or choose **VM > Replay > Record**.

A recording-specific snapshot is taken, and the recording dialog box appears to indicate that recording is in progress.

If the **Record** command is unavailable, the feature might not be enabled or the hard disk might be set to independent mode. See [“Enabling Record/Replay for a Virtual Machine”](#) on page 235.

- 3 To add a marker during recording, click **Add Marker** in the recording dialog box.
Aside from the markers you add, markers are automatically added according to the frequency you set by using the virtual machine settings editor. See [“Enabling Record/Replay for a Virtual Machine”](#) on page 235.
- 4 When you want to stop recording, click the **Stop** button in the recording dialog box or in the toolbar.
(Optional) On Windows, while making a recording you can use the minimized record control to either stop a recording or add a marker.
- 5 Complete the dialog box that appears and click **Save**.
- 6 To change the name of the recording, add or change the description, or delete the recording, choose **VM > Snapshot > Snapshot Manager**.

Replaying a Recording

To replay a recording

- 1 Select the virtual machine.
- 2 If it is powered on and you do not want to lose the current state of the virtual machine, take a snapshot of it.

For instructions, see [“Take a Snapshot”](#) on page 195.

- 3 To play the latest recording of the virtual machine, do one of the following:
 - Click the **Replay <name_of _recording>** button in the toolbar.
 - Choose **VM > Replay > Replay <name_of _recording>**.
 - On Windows, while replaying a recording you can use the controls in the minimized replay control.
- 4 To play an earlier recording, use the snapshot manager, as follows:
 - a Choose **VM > Snapshot > Snapshot Manager**.
 - b Select the recording snapshot you want to play and click **Replay**.

If you stop the recording before it is finished replaying and then click the **Play** button again, the recording starts from its beginning, not from the point where you clicked **Go Live**.

A snapshot of a recording is shown in [Figure 10-4, “Snapshot Manager on a Windows Host,”](#) on page 193.

- 5 In the dialog box that appears, confirm that you want to start replaying the recording.
- 6 To suspend the replay, click the **Pause** button in the replay control dialog box. The button toggles to a **Play** button so that you can click it again to resume playing the recording.
- 7 (Optional) To adjust the speed of a playback, click the replay speed control buttons. This control is shown in Figure 13-2.

Keep in mind that the fastest speed for replay is real time. If you press the right-arrow key when the recording is slowed down by only 10 microseconds, then it will speed up by only 10 microseconds.
- 8 (Optional) To make a trace file of events that occurred during recording, see [“Creating an Execution Trace File of a Recording”](#) on page 240.
- 9 (Optional) To stop replaying the recording before it finishes playing, click the **Go Live** button to stop the replay and resume interacting with the virtual machine.

Browsing a Recording

The length of a recording can vary from a few minutes to several hours. When the recording is several hours long, to access a specific event within the recording drag the slider to the desired position in the recording. The virtual machine reverts to the nearest previous snapshot and starts replaying until it reaches the target location.

During the replay, the slider remains at the same point and the remaining playback time appears in red above the **Current Replay Position Slider**. On Windows, you can zoom in and out of the recording using the zoom controls. On Linux, use the zoomed in auto scroll function to preview the recording. When the recording reaches the **Current Replay Position Slider** the recording is paused and the virtual machine reverts to the normal state.

Creating an Execution Trace File of a Recording

Trace files are detailed logs produced by a program that are helpful for debugging. When you make an execution trace file of a recording you can view all the events that occurred during the recording.

To create an execution trace file of a recording

- 1 Start play back of a recording, as described in [“Replaying a Recording”](#) on page 239.
- 2 To make an execution trace file of the recording click inside the virtual machine, so that keyboard events are grabbed by the virtual machine, and press the T key (“trace” key).

A trace file is created in the directory where this virtual machine’s configuration (.vmx) file is stored. The filename is `ReplayTrace-<timestamp>.gz`, where `<timestamp>` is the time at which you pressed the T key.

The speed at which the recording plays slows considerably while the trace file is being made.

- 3 To end the trace file, either press the T key again or click the **Stop** button in the **Replay** toolbar.

Otherwise, the trace file ends when the recording finishes playing.

If you press the T key to end the trace file before the recording ends and then press T again, another trace file is created.

Maintenance Tasks for Using Recordings

Depending on the length of a recording, the number of its periodic snapshots, and the number of recordings, the disk space used for the record/replay feature can be considerable. When you create recordings, Workstation goes into full debugging mode. The topics in this section provide guidance for addressing these issues.

Deleting a Recording

Recordings can consume large amounts of disk space, depending on the activities of the virtual machine and the length of the recording. Delete recordings you do not need to free disk space.

To delete a recording

- 1 Select the virtual machine.
- 2 Choose **VM > Snapshot > Snapshot Manager**.
- 3 In the snapshot manager window, select the recording you want to delete.
- 4 Right-click and choose **Delete > Recording and Children**.

If you select a recording and click the **Delete** button, the selected recording is removed and the corresponding snapshots in the recording remain intact.

Disabling Periodic Screenshots

If the recording session lasts for a long time, a significant number of screenshots are automatically created in the virtual machine directory.

NOTE Even when periodic screenshots are disabled, one screenshot is taken at the end of every recording.

To disable periodic screenshots

- 1 Add the following line to the configuration (.vmx) file for the virtual machine:

```
snapshot.periodicScreenshots = "X"
```

where X denotes the interval of screenshots taken in seconds. The default value for X is 5 seconds.
- 2 To disable periodic screenshots, change the value of X to 0.
- 3 Save and close the configuration file.

Set the Debugging Mode

Workstation has three modes for collecting debugging information: normal mode (which means that no debugging information is gathered), statistics mode, and full debugging mode. In normal mode, the virtual machine runs faster than in the other modes. As of the Workstation 6 release, you do not need to restart the virtual machine after changing the debugging mode.

For normal use, make sure you are not running in debugging mode, as described in the procedure in this section.

You might need to use one of the other modes under the following conditions:

- If the virtual machine sometimes crashes and you want to determine the cause, use full debugging mode so that you can send the debugging logs to VMware technical support.
- If, in normal mode, the virtual machine runs extremely slowly under some workloads, and you want to determine the cause, use statistics mode so that you can send the statistics file to VMware technical support.

After you generate some debugging information, run the `vm-support` script, as described in [“Reporting Problems”](#) on page 17, and send the output to VMware technical support.

When the cause and remedy for an issue have been found, return to normal mode.

To set a debugging mode

- 1 Start Workstation and select the virtual machine.
The virtual machine can be either powered on or powered off.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 Click the **Options** tab, and select **Advanced**.
- 4 In the **Settings** section, set the **Gather debugging information** control to the desired mode and click **OK**.

BETA

Configuring Teams

This chapter describes what virtual machine teams are used for, how to create them, and how to configure them. This chapter includes the following topics:

- [“Benefits of Using Teams”](#) on page 245
- [“Managing Teams”](#) on page 246
- [“Summary and Console Views for Teams and Their Virtual Machines”](#) on page 249
- [“Managing the Members of a Team”](#) on page 251
- [“Power Operations for Teams and Their Members”](#) on page 253
- [“Working with Team Networks”](#) on page 254
- [“Cloning and Taking Snapshots of Team Virtual Machines”](#) on page 257

Benefits of Using Teams

Workstation teams allow you to set up a virtual computer lab on one host computer. Use a team to power on multiple associated virtual machines with a single click.

You can use teams to do the following:

- **Virtualize multitier environments** – Start separate client, server, and database virtual machines with one click. Configure startup delay times so clients don’t submit queries before the server is ready.

Setting a startup delay between the booting of virtual machines also avoids overloading the CPU of the host.

- **Virtualize multiple-machine testing environments** – Set up a software package for QA on a virtual machine, and configure automation on other virtual machines to test the first.

- **Virtualize network performance and security** – Team virtual machines can use networking just as other virtual machines can. In addition, team members can communicate in private networks called LAN segments. Team networking lets you to do the following:
 - Isolate a team completely from the host network. A team LAN segment is undetectable and inaccessible from any other network.
 - Create a virtual DMZ or proxy server to securely bridge the team members to the outside network.
 - Allow specific network bandwidth and packet loss to each virtual machine on the team.
 - Connect all team members fully to host resources.

You control all traffic allowed between the host network and team virtual machines.

- **Monitor multiple virtual machines** – Use thumbnail views of the virtual machine displays to review activity on team virtual machines simultaneously.

Managing Teams

This section includes procedures for creating, deleting, opening, closing, and changing the names of teams.

Create a Team

Use the New Team wizard to create a team and add virtual machines.

Before creating a team, if you plan to add virtual machines to the team while completing the New Team wizard, take these actions:

- Power off any virtual machines that you want to add to the team.
- Power off any virtual machines that you want to clone if you intend to create a clone and add it to the team.

You can instead add virtual machines after you create the team, by using the **Team** menu.

NOTE Workstation version 4 virtual machines cannot be added to teams.

To create a team

- 1 From the Workstation menu bar, choose **File > New > Team**.
- 2 In the New Team wizard, supply the following information:
 - a Enter a name for the team and specify the location of the virtual team files.
By default, the team files are stored in the same directory as virtual machines. See [“Virtual Machine Location”](#) on page 88.
 - b Specify whether to add virtual machines to the team now or later.
If you want to add them now, you have the following options:
 - **New Virtual Machine** – Launches the New Virtual Machine wizard. See [“Using the New Virtual Machine Wizard”](#) on page 92.
 - **Existing Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file.
When you add a virtual machine to a team it can no longer be accessed outside the team. See [“Add a Virtual Machine to a Team”](#) on page 251.
 - **New Clone of Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file. After you select a virtual machine, Workstation launches the Clone Virtual Machine wizard. See [“Creating Clones”](#) on page 203.
 - c Specify whether to add one or more LAN segments.
You can add LAN segments after you create the team by using the **Team** menu. If you add LAN segments while creating the team, you can change default names and bandwidth later. See [“Working with Team Networks”](#) on page 254.

After the team is created, you can add it to the **Favorites** list. Use the **Team** menu to configure the team further, or to add and remove virtual machines.

Open a Team and Add It to the Favorites List

Opening a team displays its summary tab but does not power on the virtual machines included in the team.

To open a team and add it to the Favorites list

- 1 From the Workstation menu bar, choose **File > Open**.
- 2 Browse to the location of the `.vmtm` file for the team you want.

- 3 Select the file and click **Open**.

A summary tab for the team appears in the Workstation window.

- 4 (Optional) To add the team to the **Favorites** list, choose **File > Add to Favorites**.

After a team is added to the **Favorites** list, you can open it by clicking it in the **Favorites** list rather than using the menu bar.

You can now power on one or more of the virtual machines in the team. See [“Power On a Team”](#) on page 253.

Change the Name of a Team

When you create a team, the name of the directory where the team (.vmtm) file is stored is based on the name you originally give the team. Although you can change the name of the team, the name of this file does not change.

To change the name of a team

To change the name of a team, do one of the following:

- If the team is in the **Favorites** list, right-click it and choose **Rename**. Type the new name and press Enter.
- Select the team and choose **Team > Settings > Options**. Type a new name in the **Team name** field and click **OK**.

Power Off or Close a Team

Powering off a team means shutting down all the virtual machines in the team. The virtual machines are powered off in reverse order of that shown in the startup sequence. See [“Specify the Startup Sequence for a Team”](#) on page 252.

Closing a team removes its summary tab from the Workstation window. Depending on how you set Workstation preferences, closing a team might require powering off the team.

To power off or close a team

Depending on which operation you want to perform, do one of the following:

- To power off the team, select it and choose **Team > Power > Power Off**.
Depending on how you configured power operations, the guest operating system might be shut down before the virtual machine is powered off. See [“Configure Power Off and Reset Options for a Virtual Machine”](#) on page 152.
- To close the team, select it and choose **File > Close**.

Depending on how Workstation preferences are set, if any of the team's virtual machines are still powered on, you might see a prompt. For information about the options shown in the prompt, see [“Closing Virtual Machines and Exiting Workstation”](#) on page 81.

Delete a Team

Before you can delete a team, you must power off all virtual machines that are members of the team. See [“Power Off or Close a Team”](#) on page 248.

When you delete a team, you can choose to delete:

- Only the team (retaining the virtual machines in the team)
- The team and the virtual machines in the team

To remove a team from the Workstation window rather than deleting it, see [“Remove a Virtual Machine from a Team”](#) on page 251.



CAUTION Deleting a team permanently removes the team files from the host file system and removes associated LAN segments from all virtual machines. Deleting the team's virtual machines along with the team removes the virtual machine files permanently.

To delete a team

- 1 Select the team and choose **Team > Delete from Disk**.
- 2 Complete the dialog box that appears:
 - To delete the team without deleting the virtual machines in it, choose **Delete**.
 - To delete the team and the virtual machines in it, choose **Delete Team and VMs**.

When you delete a team, you also delete all team LAN segments. The virtual Ethernet adapters associated with deleted LAN segments become disconnected. Bridged, host-only, NAT, and custom configurations remain unchanged.

- 3 Click **OK**.

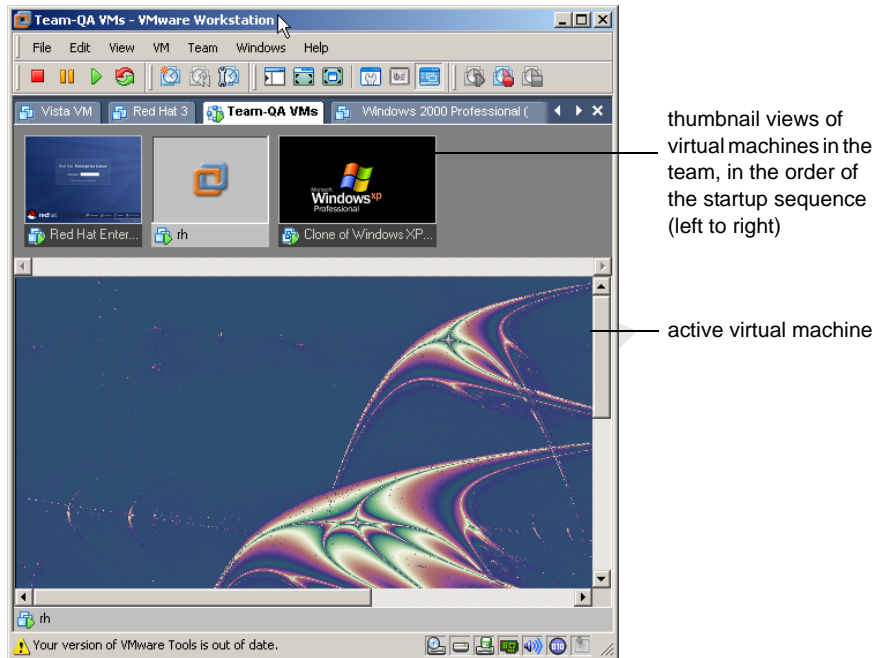
Summary and Console Views for Teams and Their Virtual Machines

Workstation displays teams in a summary view or console view:

- The summary view is available at any time. See [“Summary View”](#) on page 64.

- The console view is available only when a team is powered on. A grab bar allows you to resize the areas.

Figure 14-1. Console Window for a Team on a Windows Host



If the team contains many virtual machines, you might need to scroll the thumbnails to view all the virtual machines. The thumbnails are displayed in the same order as the team's startup sequence. The left-most virtual machine is the first one in the sequence.

Workstation updates thumbnails in real time, to display the actual content of the virtual machine screens. The active virtual machine is the one you select or switch to by using the **Team > Switch To** menu. It appears in the lower pane of the console. Its thumbnail is represented by the **VMware** icon.

Workstation menus and commands directly affect only the active virtual machine, and you can use the mouse and keyboard to interact directly with the active virtual machine.

In full screen mode, Workstation displays only the active virtual machine. See ["Use Full Screen Mode"](#) on page 156.

Managing the Members of a Team

This section includes procedures for adding virtual machines to a team, removing them from a team, and setting the order in which members of a team start and stop.

Add a Virtual Machine to a Team

Before you add a virtual machine to a team, consider these issues:

- A virtual machine is not powered on when you add it to a running team. You must power on the added virtual machine manually to use it during the current session. The added virtual machine is thereafter powered on or off with the rest of the team.
- When you add a virtual machine to a team, you can no longer operate the virtual machine outside the team. Adding a virtual machine to a team therefore removes it from the **Favorites** list.

NOTE Workstation version 4 virtual machines cannot be added to teams.

To add a virtual machine to a team

Select the team, choose **Team > Add**, and choose one of the following options:

- **New Virtual Machine** – Launches the New Virtual Machine wizard. See [“Using the New Virtual Machine Wizard”](#) on page 92.
- **Existing Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file.

When you add a virtual machine to a team it can no longer be accessed outside the team.

- **New Clone of Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file. After you select a virtual machine, Workstation launches the Clone Virtual Machine wizard. See [“Creating Clones”](#) on page 203.

Remove a Virtual Machine from a Team

Remove a virtual machine from a team when you want to use the virtual machine independently. That is, it does not need to be started up or shut down before or after any other virtual machine. It also does not need to be in a private team network.

NOTE When you remove a virtual machine from a team, you also remove it from team LAN segments. Virtual network adapters associated with LAN segments become disconnected. Bridged, host-only, NAT, and custom configurations remain unchanged.

To remove a virtual machine from a team

- 1 Power off the virtual machine that you want to remove.
- 2 Select the team and choose **Team > Remove > <virtual machine name>**.

The selected virtual machine is removed from the team.

You might want to perform these tasks after removing the virtual machine:

- Add the virtual machine to the **Favorites** list. See [“To add virtual machines and teams to the Favorites list”](#) on page 73.
- Delete the virtual machine and erase its files from the host file system. See [“Delete a Virtual Machine”](#) on page 153.

Specify the Startup Sequence for a Team

Use a startup sequence to specify the order in which virtual machines start and stop and the delay, in seconds, between starting and stopping the next virtual machine in the sequence.

Power on and resume operations occur in the order of the sequence shown in the team settings list. Power off operations occur in reverse order. The default sequence is the order in which you added the virtual machines to the team. The default delay is 10 seconds.

Setting a startup sequence is useful, for example, if you have a virtual machine that runs an application to be tested and you want it to start before the virtual machines running an automated testing script.

Setting a delay avoids overloading the CPU when multiple virtual machines start and allows applications on a virtual machine to launch before another team virtual machine attempts to connect.

To specify a startup sequence for a team

- 1 Select the team and choose **Team > Settings** and click the **Virtual Machines** tab.
- 2 Use the up and down arrow buttons to arrange the virtual machines in the list.

The virtual machine at the top of the list is the first in the startup sequence.

- 3 Select each virtual machine and specify how many seconds you want it to wait before starting the next virtual machine.

If the virtual machine team depends on precise startup timing, experiment to determine how much time the host and guest operating environments and applications need to launch.

- 4 Click **OK** to save your changes.

Power Operations for Teams and Their Members

Power operations for teams are much the same as those for an individual virtual machine. However, for a team, you can also change the sequence in which the members of a team power on and off. See [“Specify the Startup Sequence for a Team”](#) on page 252.

You can also use Workstation’s command-line application for team power operations. See [Appendix A, “Workstation Command-Line Reference,”](#) on page 455.

Power On a Team

When you power on a team, the virtual machines in the team power on in the startup sequence specified in the team settings editor. See [“Specify the Startup Sequence for a Team”](#) on page 252.

To power on a team\

Do one of the following:

- To use the Workstation GUI, select the team and choose **Team > Power > Power On**.
- To use the command line, see [“Startup Options for Workstation and Virtual Machines”](#) on page 455.

Suspend or Resume a Team

When you suspend a team, all team virtual machines start suspending simultaneously. The startup sequence determines the order in which virtual machines are resumed and how much time elapses before resuming the next team member. See [“Specify the Startup Sequence for a Team”](#) on page 252.

If you attempt to close Workstation while a team suspend or resume operation is still in progress, a warning dialog box appears.

To suspend or resume a team

- 1 To suspend or resume a team, select the team and choose one of the **Team > Power** options.

All team virtual machines start suspending simultaneously. A progress indicator appears for each team member.
- 2 To see the progress of a particular team member, choose **Team > Switch To > <virtual_machine_name>**.

The time to complete the operation varies with the size of the virtual machines.

Perform Power Operations on One Team Member

Performing a power operation for one member of a team is similar to performing the operation for a virtual machine that is not part of the team, except that instead of selecting the machine from the **Favorites** list, you select it from the team's console tab.

To perform power operations on one team member

- 1 Select the virtual machine from the team's console tab.
- 2 Choose the appropriate command from the **VM > Power** menu.

Working with Team Networks

One of the advantages of teams is the ability to isolate virtual machines in private virtual networks, called LAN segments. This can be useful with multitier testing, network performance analysis, and situations where isolation and packet loss are important.

This section focuses on LAN segments. For information about other aspects of networking, see [Chapter 15, "Configuring a Virtual Network,"](#) on page 259.

LAN Segment Requirements Regarding IP Addresses

When you add an existing virtual machine to a team, the virtual machine might be configured to expect an IP address from a DHCP server. Unlike host-only and NAT networking, LAN segments have no DHCP server provided automatically by Workstation.

Each network client must have an IP address for TCP/IP networking. Therefore you must manually configure IP addressing for team virtual machines on a LAN segment. Two choices are available:

- **DHCP** – Configure a DHCP server on your LAN segment to allocate IP addresses to your virtual machines.
- **Static IP** – Configure a fixed IP address for each virtual machine on the LAN segment.

Create a Team LAN Segment

The first step to creating a virtual network for a team is to add and name a LAN segment. You can then configure connections to this segment.

To create a team LAN segment

- 1 Select the team and choose **Team > Add > LAN Segment**.
- 2 Enter a name for the private network and click **OK**.

You can configure the other settings in this dialog box later.

You might want to perform these tasks after creating a LAN segment:

- Configure network transmission properties for the segment. See [“Configure LAN Segments”](#) on page 255.
- Create a network adapter and connect it to the segment. See [“Add or Remove Network Adapters”](#) on page 256.

Configure LAN Segments

You can configure network transmission properties for a team LAN segment, including bandwidth settings such as connection type and speed, as well as percentage of packet loss allowed.

To configure LAN segments

- 1 Select the team and choose **Team > Settings**.
- 2 Click the **LAN Segments** tab, and complete the fields.

From this tab you can add, remove, and rename the LAN segments configured for the team.

The list in the left pane displays LAN segments associated with the team.

- 3 Click a name to select the LAN segment you want to configure.

The right pane displays parameters for the physical properties of the emulated LAN segment link:

- **Name** – Name of the LAN segment. To change the name, type a new name in the **Name** field.
- **Bandwidth** – Drop-down menu of bandwidths for typical network links. To change the bandwidth, choose another connection type from the drop-down menu.
- **Kbps** – Field to set a custom bandwidth. Changes here are overwritten when you make a selection from the **Bandwidth** menu. To change the bandwidth, type a number into the field.

- **Packet Loss** – Specification of the efficiency or faultiness of the link, measured in the percentage of packets lost from the total number of packets transmitted. To change the packet loss setting, type a number into the field.
- 4 Click **OK** to save your changes.
 - 5 (Optional) If virtual machines are currently running and you want them to adopt these configuration changes, power on, reset, or resume the virtual machines, as appropriate.

Add or Remove Network Adapters

A physical PC must have a network adapter or NIC (network interface controller), for each physical network connection. Similarly, a virtual machine must be configured with a virtual network adapter for each LAN segment it interacts with.

To connect a virtual machine to multiple LAN segments simultaneously, you must configure that virtual machine with multiple network adapters.

To add or remove network adapters

- 1 Power off the virtual machine that you want to add an adapter to or remove an adapter from.
- 2 Select the team and choose **Team > Settings**.
- 3 On the **Connections** tab, select the virtual machine and do one of the following:
 - To add an adapter, click **Add Adapter**.
 The added adapter is displayed in the **Adapters** column. By default, the adapter connects to the bridged LAN segment, but you can change the setting by clicking a check box for another segment. If the segment you want to use is not listed, create it. See [“Create a Team LAN Segment”](#) on page 254.
 NICs configured with connections through a DHCP server cannot connect to a team LAN segment.
 - To remove an adapter, select the adapter you want to remove and click **Remove Adapter**.
- 4 Click **OK**.

Delete a LAN Segment

Deleting a LAN segment disconnects all virtual Ethernet adapters that are configured for that LAN segment. When you remove a virtual machine from a team, you must

manually configure its disconnected virtual Ethernet adapter if you want to reconnect the virtual machine to a network.

To delete a LAN segment

- 1 Select the team either from the **Favorites** list or by clicking the summary tab for the team.
- 2 From the Workstation menu bar, choose **Team > Settings** and click the **LAN Segments** tab.
- 3 Select the LAN segment you want to delete.
- 4 Click **Remove**, and click **OK**.

Cloning and Taking Snapshots of Team Virtual Machines

You can clone a virtual machine in a team in the same way you clone any other virtual machine. See [“Creating Clones”](#) on page 203.

When you clone a virtual machine in a team:

- The resulting clone is not part of the team.
- The clone appears on the **Favorites** list as well as in a summary window.
- If the parent virtual machine is configured for a LAN segment, the virtual Ethernet adapter for that LAN segment on the clone is disconnected. To connect to a network, you must reconfigure the virtual Ethernet adapter manually.

Snapshots operate on virtual machines, not on the whole team. When a team is active, the **Snapshot** button on the toolbar takes a snapshot of only the active virtual machine.

To preserve the state of all virtual machines on a team, power off the team, and take a snapshot of each virtual machine before you power on the team again.

BETA

Configuring a Virtual Network

15

This chapter previews the virtual networking components that VMware Workstation provides and shows how to use them with your virtual machine. This chapter includes the following topics:

- [“Components of the Virtual Network”](#) on page 259
- [“Common Networking Configurations”](#) on page 260
- [“Example of a Custom Networking Configuration”](#) on page 265
- [“Changing a Networking Configuration”](#) on page 267
- [“Configuring Bridged Networking”](#) on page 269
- [“Changing the Subnet or DHCP Settings for a Virtual Network”](#) on page 272
- [“Configuring Host Virtual Network Adapters”](#) on page 275

Components of the Virtual Network

VMware Workstation provides the bridged, network address translation (NAT), host-only, and custom networking options to configure a virtual machine for virtual networking. The following sections describe the devices that make up a virtual network.

Virtual Switch

Like a physical switch, a virtual switch lets you connect other networking components together. Virtual switches are created as needed by Workstation, up to a total of 10 virtual switches on Windows and 255 on Linux. You can connect one or more virtual machines to a switch.

By default, a few of the switches and the networks associated with them are used for special named configurations:

- The bridged network uses vmnet0, as described in [“Bridged Networking”](#) on page 261.
- The NAT network uses vmnet8, as described in [“Network Address Translation \(NAT\)”](#) on page 262.
- The host-only network uses vmnet1, as described in [“Host-Only Networking”](#) on page 263.

The other available networks are named vmnet2, vmnet3, vmnet4, and so on.

DHCP Server

The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in configurations that are not bridged to an external network. For example, host-only and NAT configurations use the DHCP server.

Network Adapter

One virtual network adapter is set up for your virtual machine when you create it with the New Virtual Machine wizard using any type of networking. It appears in the guest operating system as an AMD PCNET PCI adapter or as an Intel Pro/1000 MT Server Adapter. On Windows Vista guests, it is an Intel Pro/1000 MT Server Adapter.

You can create and configure up to 10 virtual network adapters in each Workstation 6.5 virtual machine by using the virtual machine settings editor. The limit is three adapters for Workstation 4 or 5 virtual machines. For more information, see [“Changing a Networking Configuration”](#) on page 267.

Common Networking Configurations

The following sections illustrate the networking configurations that are set up for you automatically when you choose the standard networking options in the New Virtual Machine wizard or the virtual machine settings editor.

If you select the Typical setup path in the New Virtual Machine wizard, the wizard sets up bridged networking for the virtual machine. Select the Custom setup path to choose any of the other common configurations: bridged networking, network address translation (NAT), and host-only networking. The wizard connects the virtual machine to the appropriate virtual network.

You can set up more specialized configurations by choosing the appropriate settings in the virtual machine settings editor, in the virtual network editor (on Windows hosts), and on your host computer.

On a Windows host, the software needed for all networking configurations is installed when you install Workstation. On a Linux host, when you install and configure Workstation, you can choose whether to have bridged, host-only, and NAT networking available to your virtual machines. You must choose all options during configuration to make all networking configurations available for your virtual machines.

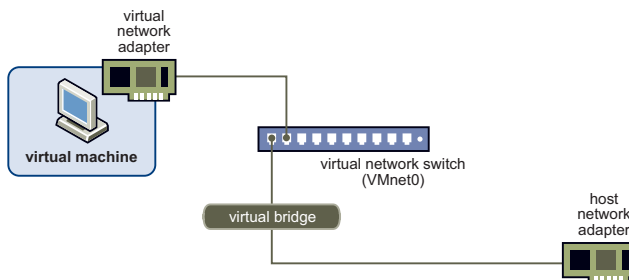
Only one virtual machine is shown in each example, but multiple virtual machines can be connected to the same virtual Ethernet switch. On a Windows host, you can connect an unlimited number of virtual network devices to a virtual switch. On a Linux host, you can connect up to 32 devices.

Bridged Networking

Bridged networking connects a virtual machine to a network by using the host computer's network adapter. If your host computer is on a network, this is often the easiest way to give your virtual machine access to that network. The virtual network adapter in the virtual machine connects to the physical network adapter in your host computer, allowing it to connect to the LAN used by the host computer.

Bridged networking configures your virtual machine as a unique identity on the network, separate from and unrelated to its host. It makes the virtual machine visible to other computers on the network, and they can communicate directly with the virtual machine. Bridged networking works with Ethernet, DSL, wireless cards, and legacy phone modems.

Figure 15-1. Bridged Networking Setup



How to Set Up Bridged Networking

Bridged networking is set up automatically if you select **Use bridged networking** in the New Virtual Machine wizard or if you select the Typical setup path. You can set up additional virtual bridges for custom configurations that require connections to more than one physical network adapter on the host computer. Linux and Windows hosts can use bridged networking to connect to both wired and wireless networks.

Set Up Requirements for IP Addresses

If you use bridged networking, your virtual machine must have its own identity on the network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for your virtual machine and which networking settings you should use in the guest operating system. Generally, your guest operating system can acquire an IP address and other network details automatically from a DHCP server, or you might need to set the IP address and other details manually in the guest operating system.

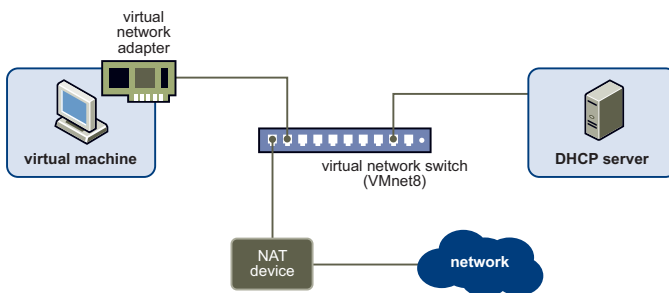
If you use bridged networking, the virtual machine is a full participant in the network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

NOTE If the host computer is set up to boot multiple operating systems and you run one or more of them in virtual machines, you need to configure each operating system with a unique network address.

Users who boot multiple operating systems often assign all systems the same address, since they assume only one operating system will be running at a time. If you use one or more of the operating systems in a virtual machine, this assumption is no longer true.

Network Address Translation (NAT)

Configures your virtual machine to share the IP and MAC addresses of the host. The virtual machine and the host share a single network identity that is not visible outside the network. NAT can be useful when you are allowed a single IP address or MAC address by your network administrator. If you are not able to give your virtual machine an IP address on the external network, you can use NAT to give your virtual machine access to the Internet or other TCP/IP network. NAT uses the host computer's network connection. NAT works with Ethernet, DSL, and legacy phone modems.

Figure 15-2. Network Address Translation Setup

If you select NAT, the virtual machine can use many standard TCP/IP protocols to connect to other machines on the external network. For example, you can use HTTP to browse Web sites, FTP to transfer files, and Telnet to log on to other computers. NAT also allows you to connect to a TCP/IP network using a Token Ring adapter on the host computer.

In the default configuration, computers on the external network cannot initiate connections to the virtual machine. That means, for example, that the default configuration does not let you use the virtual machine as a Web server to send Web pages to computers on the external network. This configuration has the advantage of protecting the guest operating system from being compromised before you have a chance to install security software. For example, it is often recommended that for Windows guest operating systems, you use NAT until you install antivirus software.

How to Set Up NAT

A NAT connection is set up automatically if you select the Custom setup in the New Virtual Machine wizard and select **Use network address translation**.

Set Up Requirements for IP Addresses

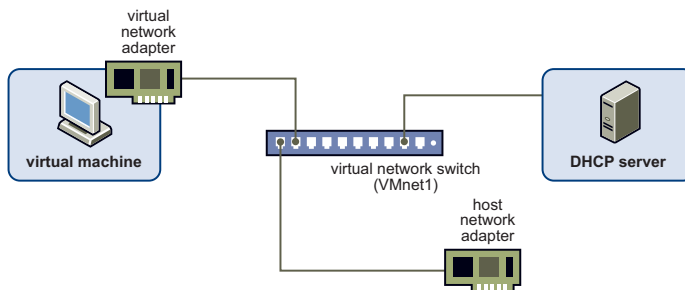
If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

Host-Only Networking

Host-only networking creates a network that is completely contained within the host computer. Host-only networking provides a network connection between the virtual

machine and the host computer, using a virtual network adapter that is visible to the host operating system. This approach can be useful if you need to set up an isolated virtual network. In this configuration, the virtual machine cannot connect to the Internet.

Figure 15-3. Host-Only Networking Setup



How to Set Up Host-Only Networking

A host-only network is set up automatically if you select the Custom setup in the New Virtual Machine wizard and select **Use host-only networking**.

Set Up Requirements for IP Addresses

If you use host-only networking, your virtual machine and the host virtual adapter are connected to a private Ethernet network. Addresses on this network are provided by the VMware DHCP server.

Routing and Connection Sharing

If you install the proper routing or proxy software on your host computer, you can establish a connection between the host virtual network adapter and a physical network adapter on the host computer. This allows you, for example, to connect the virtual machine to a Token Ring or other non-Ethernet network.

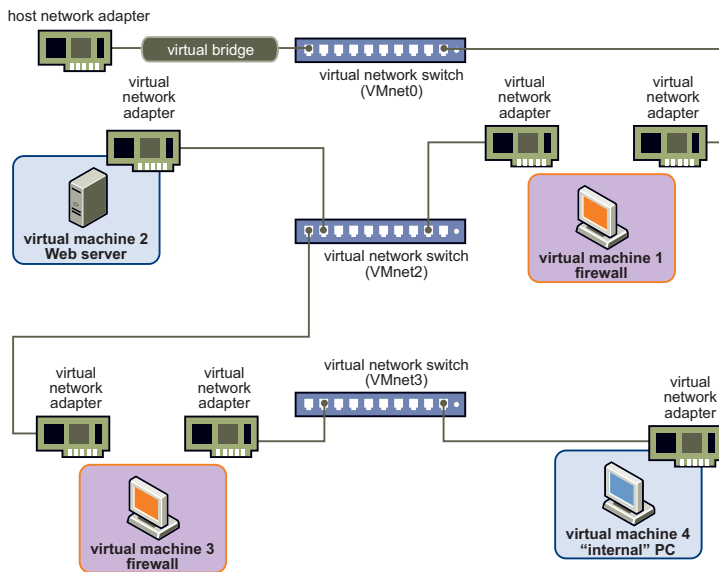
On a Windows 2000, Windows XP, or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the host's dial-up networking adapter or other connection to the Internet. See your Windows documentation for details on configuring Internet connection sharing.

Example of a Custom Networking Configuration

The virtual networking components provided by Workstation make it possible for you to create sophisticated virtual networks. The virtual networks can be connected to one or more external networks, or they can run entirely on the host computer. On Windows hosts, you can use the virtual network editor to access multiple network cards in your host and create multiple virtual networks.

Before attempting to set up complex virtual networks, you should have a good understanding of how to configure network devices in your host and guest operating systems. The example described in this section illustrates most of the ways you can combine devices on a virtual network. Other custom configurations are described in [“Advanced Virtual Networking”](#) on page 277 and [“Using NAT”](#) on page 292. In this configuration, a Web server connects through a firewall to an external network. An administrator’s computer connects to the Web server through a second firewall.

Figure 15-4. Custom Configuration That Uses Two Firewalls



Set Up a Custom Networking Configuration

To set up the custom networking configuration, you need to create four virtual machines and use the virtual machine settings editor to adjust the settings for their virtual network adapters. You also need to install the appropriate guest operating

systems and application software in each virtual machine and make the appropriate networking settings in each virtual machine.

To set up a custom networking configuration

- 1 Set up four virtual machines using the New Virtual Machine wizard:
 - a To open this wizard, choose **File > New > Virtual Machine**.
 - b Create the first virtual machine with bridged networking so it can connect to an external network by using the host computer's network adapter.
 - c Create the other three virtual machines without networking.

You will set up their virtual network adapters in later steps and install the operating systems in [Step 6](#).
- 2 Configure network settings for the first and second virtual machines:
 - a Open virtual machine, but do not power it on.
 - b Use the virtual machine settings editor to add a second virtual network adapter.

See ["Changing a Networking Configuration"](#) on page 267.
 - c Connect the second adapter to Custom (vmnet2).
- 3 Configure network settings for the third virtual machine:
 - a Open virtual machine 3, but do not power it on.
 - b Use the virtual machine settings editor to add a virtual network adapter.

See ["Changing a Networking Configuration"](#) on page 267.
 - c Connect the second adapter to Custom (vmnet2).
 - d Use the virtual machine settings editor to add a second virtual network adapter.
 - e Connect the adapter to Custom (vmnet3).
- 4 Configure network settings for the fourth virtual machine:
 - a Open virtual machine 4, but do not power it on.
 - b Use the virtual machine settings editor to add a virtual network adapter.

See ["Changing a Networking Configuration"](#) on page 267.
 - c Connect the second adapter to Custom (vmnet3).
- 5 Determine the network addresses used for vmnet2 and vmnet3:

- On Windows hosts, open a command prompt and run:
`ipconfig /all`
 Note the network addresses used by each virtual adapter.
 - On Linux hosts, open a terminal and run:
`ifconfig`
 Note the network addresses used by each virtual switch.
- 6 Power on each virtual machine in turn and install the appropriate guest operating system.
 - 7 On a Windows host, you are not required to configure network addresses manually. You can instead use Workstation's DHCP server.
 - a From the Workstation menu bar, choose **Edit > Virtual Network Settings > DHCP**.
 - b Add vmnet2 and vmnet3 to the list of virtual networks served by the virtual DHCP server.
 - 8 Configure the networking in each guest operating system:
 - **Machine 1** – For the bridged network adapter in virtual machine 1, use the networking settings needed for a connection to the external network. If the virtual machine gets its IP address from a DHCP server on the external network, the default settings should work.
 For the second network adapter in virtual machine 1, manually assign an IP address in the range you are using with vmnet2.
 - **Machine 2** – Assign an IP address in the range you are using with vmnet2.
 - **Machine 3** – Network adapters are connected to vmnet2 and vmnet3. Assign each adapter an IP address in the range you are using with the virtual network to which it is connected.
 - **Machine 4** – Assign an IP address in the range you are using with vmnet3.
 - 9 Install the necessary application software in each virtual machine.

Changing a Networking Configuration

This section describes how you can find out the type of network a virtual machine is using, use the virtual machine settings editor to add virtual network adapters to your virtual machine, and change the configuration of existing adapters.

Find the Network Type of a Virtual Machine

Unless you set up a custom network connection, a virtual machine uses a bridged, NAT (network address translation), or host-only network connection. If you create a virtual machine by using the Typical setup path in the New Virtual Machine wizard, the virtual machine is created using the NAT network type.

For more information, see [“Common Networking Configurations”](#) on page 260.

To find the network type of a virtual machine

- 1 Select the virtual machine.
- 2 Choose **VM > Settings > Hardware**.
- 3 Select the network adapter.

The **Network Connection** section displays the details that allows you to change the settings.

If you want to change the network type, see [“Modify Existing Virtual Network Adapters”](#) on page 269.

Add Virtual Network Adapters

Before you begin, determine the network type you want to use. See [“Common Networking Configurations”](#) on page 260.

To add new virtual network adapters

- 1 Power off the virtual machine to which you want to add the adapter.
- 2 Choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 On the **Hardware** tab, click **Add**.
The Add Hardware wizard starts.
- 4 Select **Network adapter** and click **Next**.
- 5 Select the network type you want to use.
- 6 (Optional) If you select **Custom**, choose the vmnet network you want to use from the drop-down list.

Although vmnet0, vmnet1, and vmnet8 are technically available in this list, they are normally used for bridged, host-only, and NAT configurations, respectively.

Special steps are required to make them available for use in custom configurations. You should choose one of the other switches.

- 7 Click **Finish**.

The new adapter is added.

- 8 Click **OK** to save your configuration and close the virtual machine settings editor.

Modify Existing Virtual Network Adapters

Before you begin, determine the network type you want to use. See [“Common Networking Configurations”](#) on page 260.

To modify existing virtual network adapters

- 1 Select the virtual machine.
The virtual machine can be either powered on or powered off.
- 2 From the Workstation menu bar, choose **VM > Settings**.
- 3 On the **Hardware** tab, select the adapter you want to modify.
- 4 Select the network type you want to use.
- 5 (Optional) If you select **Custom**, choose the vmnet virtual network you want to use for the network from the drop-down list.

Although vmnet0, vmnet1, and vmnet8 are technically available in this list, they are normally used for bridged, host-only, and NAT configurations, respectively. Special steps are required to make them available for use in custom configurations. You should choose one of the other switches.

- 6 Click **OK** to save your changes and close the virtual machine settings editor.
- 7 Be sure the guest operating system is configured to use an appropriate IP address on the new network.

If the guest is using DHCP, release and renew the lease. If the IP address is set statically, be sure the guest has an address on the correct virtual network.

Configuring Bridged Networking

Although the user interface for the virtual network editor is somewhat different on Windows and Linux host, both allow you to configure bridged networking. You can view and change the settings for bridged networking on your host, determine which network adapters on your host to use for bridged networking, and map specific

network adapters to specific virtual networks, called vmnets. The changes you make to bridged networking affect all virtual machines using bridged networking on the host.

Configure vmnet0 Bridged Networking on a Windows Host

To configure vmnet0 bridged networking on a Windows host

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
The virtual network editor appears, with the **Summary** tab active.
By default, vmnet0 is set to use automatic bridging mode and bridges to one of the active network adapters on the host computer.
- 2 Click the **Automatic Bridging** tab, and select the check box for **Automatically choose an available physical adapter**.
On host systems with more than one physical network adapter installed, the choice of which adapter Workstation uses is arbitrary. If you want to place restrictions on the choice, see [“Add or Remove a Host Network Adapter from the List of Excluded Adapters.”](#)
- 3 Click **OK** to save your changes and close the virtual network editor.

Add or Remove a Host Network Adapter from the List of Excluded Adapters

To add or remove a host network adapter from the list of excluded adapters

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **Automatic Bridging** tab.
- 3 In the **Excluded adapters** section, do one of the following:
 - To remove an adapter, select the adapter and click **Remove**.
 - To add an adapter, click **Add**. In the Add Excluded Adapters dialog box, select the listing for the adapter you want to add and click **OK**.
- 4 Click **OK** to save your changes and close the virtual network editor.

Designate a Physical Network Adapter to Bridge to Custom Virtual Switches

Before you change the bridged adapter mappings make sure to check which virtual network the physical network adapter is going to be assigned to.



CAUTION If you reassign a physical network adapter to a different virtual network, any virtual machine using the original network loses its network connectivity through that network. You must then change the setting for each affected virtual machine's network adapter individually.

This can be especially troublesome if your host has only one physical network adapter and you reassign it to a vmnet other than vmnet0. In this case, even though the vmnet still appears to be bridged to an automatically chosen adapter, the only adapter it can use has been assigned to another vmnet.

To designate a physical network adapter to bridge to custom virtual switches

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **Host Virtual Network Mapping** tab.
- 3 Choose an adapter from the drop-down list beside the name of the virtual switch you want to use.

You can create a custom bridged network on virtual switches vmnet2 to vmnet7. On Windows, you can also use vmnet9. On Linux, you can also use vmnet10 through vmnet255.

- 4 Click **OK** to save your changes and close the virtual network editor.

Configure vmnet0 Automatic Bridged Networking on a Linux Host

To configure vmnet0 automatic bridged networking on a Linux host

- 1 On the Linux host, do one of the following:
 - From the desktop, choose **Applications > System Tools > VMware Network Configuration**, or the equivalent menu path for your version of Linux.
 - Open a terminal window and enter the following command:

```
/usr/bin/vmware-netcfg
```

- 2 When prompted, enter the administrator password.

The virtual network editor appears. By default, vmnet0 is set to use automatic bridging mode and bridges to one of the active network adapters on the host computer.

- 3 If the table in the network editor does not display a row for vmnet0, click **Add Network** and complete the Add Virtual Network dialog box.

- 4 Select the vmnet0 row in the table and verify that the **Bridged** radio button is selected.
- 5 Do one of the following:
 - If you want to use automatic bridging, click **Automatic Settings** and complete the dialog box.

If you select more than one check box, the virtual machine bridges to the first available host network adapter (NIC). If an item in the list is disabled, the adapter is not available because it is already being used to bridge to another vmnet.
 - If you want to specify one host network adapter, use the **Bridge to** list box.
- 6 Click **Save** to save your changes and close the virtual network editor.

Changing the Subnet or DHCP Settings for a Virtual Network

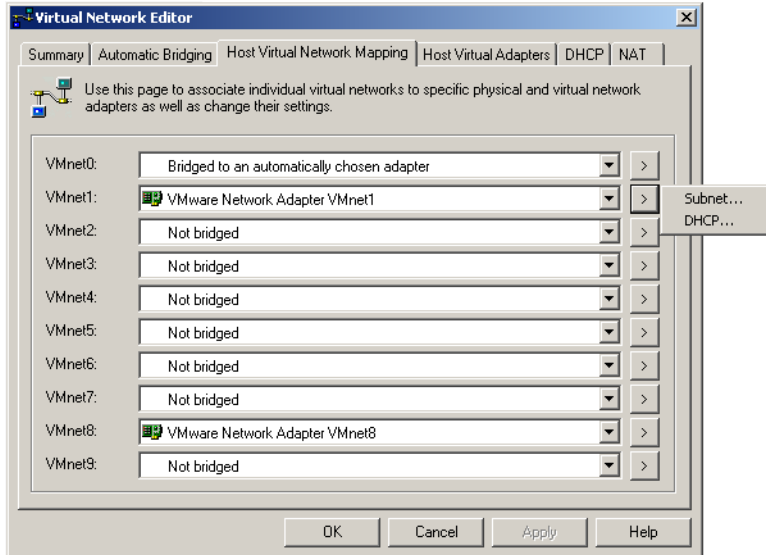
On Windows and Linux hosts, you can use the virtual network editor to make changes to subnet and DHCP settings.

Change Subnet or DHCP Settings on a Windows Host

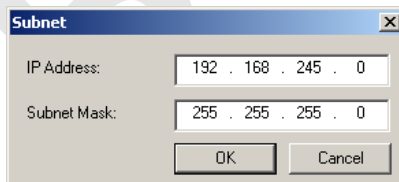
To change subnet or DHCP settings on a Windows host

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **Host Virtual Network Mapping** tab.

- 3 Click the button on the right that corresponds to the virtual network you want to configure.



- 4 Choose **Subnet** or **DHCP**:
 - In the Subnet dialog box, you can change the subnet's IP address and the subnet mask.



The address should specify a valid network address that is suitable for use with the subnet mask.

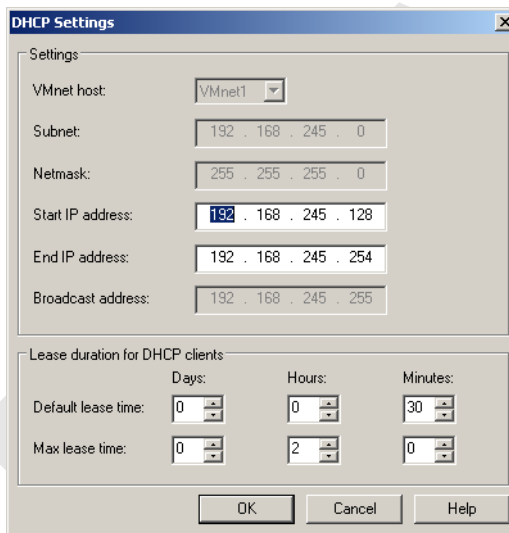
The default subnet mask is 255.255.255.0 (a class-C network). Typically, this means you should modify only the third number in the IP address—for example, x in 192.168.x.0 or 172.16.x.0. In general, you should not change the subnet mask. Certain virtual network services might not work as well with a customized subnet mask.

When you modify the network address or subnet mask, Workstation automatically updates the IP address settings for other components such as

DHCP, NAT, and host virtual adapter if the default settings have never been changed. The specific settings that are automatically updated include DHCP lease range, DHCP server address, NAT gateway address, and host virtual adapter IP address.

However, if you have changed any of these settings from its default value, Workstation does not update that setting automatically. Workstation presumes that custom settings are not to be modified. This is the case even if you later changed the setting back to the default.

- In the DHCP settings dialog box, you can change the range of IP addresses provided by the Workstation DHCP server on a particular virtual network.



You can also use this dialog box to set the duration of DHCP leases provided to clients on the virtual network.

- 5 Click **OK** to save your changes and close the virtual network editor.

Change Subnet or DHCP Settings on a Linux Host

NAT and host-only network types can have settings for subnet IP. You can use the virtual network editor to change subnet settings for a virtual network on a Linux host.

You can also use the virtual network editor to specify that a local DHCP service distributes IP addresses to virtual machines. To change DHCP settings further, edit the `dhcp.conf` file. See [“Configuring the DHCP Server on a Linux Host”](#) on page 279.

To change subnet or DHCP settings on a Linux host

- 1 On the Linux host, do one of the following:
 - From the desktop, choose **Applications > System Tools > VMware Network Configuration**, or the equivalent menu path for your version of Linux.
 - Open a terminal window and enter the following command:
`/usr/bin/vmware-netcfg`
- 2 When prompted, enter the administrator password.
 The virtual network editor appears.
- 3 If the table in the network editor does not display a row for the network type you want, click **Add Network** and complete the Add Virtual Network dialog box.
 Use vmnet1 for a host-only network type, and use vmnet8 for a NAT network type.
- 4 In the virtual network editor, select the row in the table that corresponds to the network you want to edit and verify that the **NAT** radio button or the **Host-only** radio button is selected, as appropriate.
- 5 Use the appropriate check boxes to specify whether you want to use a DHCP service, a host virtual adapter, or both.
- 6 To specify subnet IP, do one of the following and click **Save**:
 - To automatically select an unused subnet IP, leave the **Subnet IP** text box empty.
 The next time you start the virtual network editor, the subnet IP appears in the text box.
 - Type the subnet IP you want to use in the **Subnet IP** text box.

Configuring Host Virtual Network Adapters

When you install Workstation, two network adapters are added to the configuration of your host operating system. One allows the host to connect to the host-only network, and one allows the host to connect to the NAT network.

If you are not using a virtual network adapter, you can remove it. On a Windows host, you can also disable an adapter.

The presence of virtual network adapters has a slight performance cost, because broadcast packets must go to the extra adapters. On Windows networks, browsing your network might be slower than usual. And in some cases, these adapters interact with the host computer's networking configuration in undesirable ways.

Enable or Disable a Host Virtual Adapter

To enable or disable a host virtual adapter

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **Host Virtual Adapters** tab.
- 3 Select the adapter you want to enable or disable.
- 4 Click **Disable** or **Enable**, as appropriate.
- 5 Click **OK** to save your changes and close the virtual network editor.

Add or Remove a Host Virtual Adapter

You can add a virtual network and specify which virtual or physical adapter to associate with it.

By default, the following virtual network mappings are used:

- The vmnet0 virtual network uses the bridged network type.
- The vmnet1 virtual network uses the host-only network type.
- The vmnet8 virtual network uses the NAT network type.

To add or remove a host virtual adapter

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **Host Virtual Adapters** tab.
- 3 To add an adapter, do the following:
 - a Click **Add**.
 - b In the Add Network Adapter dialog box, choose the virtual network on which you want to use the adapter and click **OK**.
- 4 To remove an adapter, select the adapter you want to remove and click **Remove**.
- 5 Click **OK** to save your changes and close the virtual network editor.

Advanced Virtual Networking

16

This chapter provides detailed information on networking capabilities and specialized configurations. This chapter includes the following advanced virtual networking topics:

- [“Selecting IP Addresses on a Host-Only Network or NAT Configuration”](#) on page 277
- [“Avoiding IP Packet Leakage in a Host-Only Network”](#) on page 280
- [“Maintaining and Changing the MAC Address of a Virtual Machine”](#) on page 282
- [“Controlling Routing Information for a Host-Only Network on Linux”](#) on page 284
- [“Potential Issues with Host-Only Networking on Linux”](#) on page 285
- [“Set Up a Second Bridged Network Interface on a Linux Host”](#) on page 286
- [“Setting Up Two Separate Host-Only Networks”](#) on page 286
- [“Set Up Routing Between Two Host-Only Networks”](#) on page 290
- [“Using Virtual Network Adapters in Promiscuous Mode on a Linux Host”](#) on page 292
- [“Using NAT”](#) on page 292
- [“Advanced NAT Configuration”](#) on page 295
- [“Using Samba with Workstation”](#) on page 305

Selecting IP Addresses on a Host-Only Network or NAT Configuration

The host and all virtual machines configured for host-only networking are connected to the network through a virtual switch. Typically, all the parties on this network use the TCP/IP protocol suite, although other communication protocols can be used.

A network address translation (NAT) configuration also sets up a private network, which must be a TCP/IP network. The virtual machines configured for NAT are connected to that network through a virtual switch.

The host computer is also connected to the private network used for NAT by a host virtual adapter.

Each virtual machine and the host must be assigned addresses on the private network. This is typically done using the DHCP server that comes with Workstation. This server does not service virtual (or physical) machines residing on bridged networks.

Addresses can also be assigned statically from a pool of addresses that are not assigned by the DHCP server.

How the Subnet Number Is Assigned

When host-only networking is enabled at the time Workstation is installed, the subnet IP address for the virtual network is automatically selected as an unused private subnet IP address. A NAT configuration also uses an unused private network automatically selected when you install Workstation.

Find the Network Type Used on a Virtual Machine

To find the network type used on a virtual machine

Do one of the following:

- On a Windows host, from the Workstation menu bar, choose **Edit > Virtual Network Settings**.

The **Summary** tab displays the subnet number associated with the virtual network.

- On a Linux host, run `ifconfig` in a terminal window.

Determining Whether to Use DHCP or Statically Assign Addresses

Using DHCP to assign IP addresses is simpler and more automatic than statically assigning them. Most Windows operating systems, for example, come preconfigured to use DHCP at boot time, so Windows virtual machines can connect to the network the first time they are booted, without additional configuration. If you want your virtual machines to communicate with each other using names instead of IP addresses, however, you must set up a naming convention, a name server on the private network, or both. In that case it might be simpler to use static IP addresses.

In general, if you have virtual machines you intend to use frequently or for extended periods of time, it is probably most convenient to assign them static IP addresses or configure the VMware DHCP server to always assign the same IP address to each of these virtual machines.

Configuring the DHCP Server on a Linux Host

On a Linux host, you configure the host-only DHCP server by editing the DHCP configuration file for vmnet1 (`/etc/vmware/vmnet1/dhcp/dhcp.conf`). To configure the DHCP server for the NAT network, edit the configuration file for vmnet8 (`/etc/vmware/vmnet8/dhcp/dhcp.conf`).

NOTE When you configure Workstation by running the `vmware-config.pl` file, all edits made to the `*.dhcp.conf` files are lost.

Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the manual pages `dhcpd(8)` and `dhcpd.conf(8)`.

Configure the DHCP Server on a Windows Host

On a Windows host, use the virtual network editor to configure the DHCP server.

To configure the DHCP server on a Windows host

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Click the **DHCP** tab.
- 3 Select the virtual network for which you want to change settings and click **Properties**.
- 4 In the DHCP Settings dialog box that appears, make changes and click **OK**.

DHCP Conventions for Assigning IP Addresses

For virtual machines that you do not expect to keep for long, use DHCP and let it allocate an IP address.

For each host-only or NAT network, the available IP addresses are split up using the conventions shown in [Table 16-1](#) and [Table 16-2](#), where `<net>` is the network number assigned to your host-only or NAT network. Workstation always uses a Class C address for host-only and NAT networks.

Table 16-1. Address Use on a Host-Only Network

Range	Address Use	Example
<net>.1	Host machine	192.168.0.1
<net>.2–<net>.127	Static addresses	192.168.0.2–192.168.0.127
<net>.128–<net>.253	DHCP-assigned	192.168.0.128–192.168.0.253
<net>.254	DHCP server	192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Table 16-2. Address Use on a NAT Network

Range	Address Use	Example
<net>.1	Host machine	192.168.0.1
<net>.2	NAT device	192.168.0.2
<net>.3–<net>.127	Static addresses	192.168.0.3–192.168.0.127
<net>.128–<net>.253	DHCP-assigned	192.168.0.128–192.168.0.253
<net>.254	DHCP server	192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Avoiding IP Packet Leakage in a Host-Only Network

By design, each host-only network should be confined to the host machine on which it is set up. That is, no packets sent by virtual machines on this network should leak out to a physical network attached to the host. Packet leakage can occur only if a machine actively forwards packets. It is possible for the host machine or any virtual machine running on the host-only network to be configured in a way that permits packet leakage.

Packet Leakage in Virtual Machines

Virtual machines might leak packets if for example, you use dial-up networking support in a virtual machine and packet forwarding is enabled, host-only network traffic might leak out through the dial-up connection. To prevent the leakage, be sure packet forwarding is disabled in your guest operating system.

Using Filtering

If the host computer has multiple network adapters, it might be intentionally configured to do IP forwarding. If that is the case, you do not want to disable

forwarding. To avoid packet leakage, you must enable a packet filtering facility and specify that packets from the host-only network should not be sent outside the host computer. Consult your operating system documentation for details on how to configure packet filtering.

Disable Packet Forwarding on Windows Hosts

Systems using server versions of Windows operating systems are capable of forwarding IP packets that are not addressed to them. By default, however, these systems and Windows Vista systems come with IP packet forwarding disabled. IP forwarding is not an issue on Windows 2000 Professional, Windows XP Professional, or Windows XP Home Edition hosts.

If you find packets leaking out of a host-only network on a Windows host computer, check to see if forwarding has been enabled on the host machine. If it is enabled, disable it.

To disable packet forwarding on Windows host

Do one of the following:

- Stop the Routing and Remote Access service:
 - a Choose **Start > Run**, and then enter **services.msc** in the Run dialog box.
 - b In the Services window that appears, disable the Routing and Remote Access service.
- Use Windows Administrative Tools to disable routing and remote access:
 - a On a Windows 2000 or Windows 2003 Server host, choose **Start > Programs > Administrative Tools > Routing and Remote Access**.
 An icon on the left is labeled with the host name. If a green dot appears over the icon, IP forwarding is turned on.
 - b To turn off IP forwarding, right-click the icon and disable **Routing and Remote Access**.
 A red dot appears, indicating that IP forwarding is disabled.

Install Windows 2000 Administrative Tools on a Local Computer

Windows 2000 Administrative Tools are not installed on a Windows 2000 Professional system. However, you can install these tools from a Windows 2000 Server or Windows 2000 Advanced Server CD-ROM.

To install Windows 2000 Administrative Tools on a local computer

- 1 Open the i386 folder on the applicable Windows 2000 Server disc.
- 2 Double-click the `adminpak.msi` file, and follow the instructions that appear in the Windows 2000 Administrative Tools Setup wizard.
- 3 After Windows 2000 Administrative Tools are installed, you can access most of the server administrative tools by choosing **Start > Programs > Administrative Tools**.

Disable Packet Forwarding on Linux Host

If you find packets leaking out of a host-only network on a Linux host computer, see whether forwarding has mistakenly been enabled on the host machine. If it is enabled, disable it.

To disable packet forwarding on Linux host

Depending on which type of Linux system you have, use one of the following methods:

- Disable forwarding by writing a 0 (zero) to the special file `/proc/sys/net/ipv4/ip_forward`. As root (`su-`), enter this command:

```
echo "0" > /proc/sys/net/ipv4/ip_forward
```
- Use a configuration option that is appropriate for your Linux distribution. For example, you might use a control panel, specify a setting at the time you compile your kernel, or possibly enter a specification when you boot your system. Consult your operating system documentation for details on the method to use with your particular distribution.

Maintaining and Changing the MAC Address of a Virtual Machine

When a virtual machine is powered on, Workstation assigns each of its virtual network adapters an Ethernet MAC (media access control) address. A MAC address is the unique address assigned to each Ethernet network device.

The software guarantees that virtual machines are assigned unique MAC addresses within a given host system. The virtual machine is assigned the same MAC address every time it is powered on if both of the following conditions are true:

- The virtual machine is not moved. That is, the path name and filename for the virtual machine's configuration file remain the same.
- No changes are made to certain settings in the configuration file.

However, Workstation cannot guarantee to automatically assign unique MAC addresses for virtual machines that run on multiple host systems.

Avoiding MAC Address Changes

To avoid changes in the MAC address automatically assigned to a virtual machine, do not move the virtual machine's configuration file. Moving it to a different host computer or even moving it to a different location on the same host computer changes the MAC address.

Also do not change certain settings in the virtual machine's configuration (.vmx) file. If you never edit the configuration file by hand and do not remove the virtual network adapter, these settings remain unchanged. If you do edit the configuration file by hand, do not remove or change the following options:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
uuid.location
uuid.bios
ethernet[n].present
```

In these options, [n] is the number of the virtual network adapter, for example 0.

NOTE To preserve a virtual network adapter's MAC address, you also must be careful not to remove the adapter. If you remove the adapter but later re-create it, the adapter might receive a different MAC address.

Manually Assigning a MAC Address

To guarantee that the same MAC address is assigned to a given virtual machine every time you power it on, even if the virtual machine is moved, or if you want to guarantee a unique MAC address for each virtual machine within a networked environment, you can assign the address manually instead of allowing Workstation to assign it.

To assign the same unique MAC address to any virtual machine manually, use a text editor to remove three lines from the configuration (.vmx) file and add one line. On a Linux host, a virtual machine created with an earlier VMware product might have a configuration file with a .cfg extension.

Remove the three lines that begin with the following from the configuration file:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
```

In these options, [n] is the number of the virtual network adapter, for example, ethernet0.

Add the following line to the configuration file:

```
ethernet[n].address = 00:50:56:XX:YY:ZZ
```

In this line, the fourth pair of numbers, XX, must be a valid hexadecimal number between 00h and 3Fh, and YY and ZZ must be valid hexadecimal numbers between 00h and FFh. You must use the above format because Workstation virtual machines do not support arbitrary MAC addresses. Place this line above the UUID lines in the file.

If you choose a value for XX:YY:ZZ that is unique among your hard-coded addresses, conflicts between the automatically assigned MAC addresses and the manually assigned addresses should never occur.

Controlling Routing Information for a Host-Only Network on Linux

A host-only network is a full-fledged network. It has a network interface associated with it (vmnet1) that is marked “up” at the time the host operating system is booted. Consequently, routing server processes that operate on the host operating system, such as **routed** and **gated**, automatically discover it and propagate information on how to reach it unless you explicitly configure them not to do so.

If either of these programs is being run only to receive routing information, the easiest solution is to run it with a **-q** option so that it does not supply routing information but only receives it.

If, however, routing services are running because they are to supply routing information, you need to configure them so they do not advertise routes to the host-only network.

The version of **routed** that comes with many distributions of Linux has no support for specifying that an interface should not be advertised. Consult the **routed(8)** manual page for your system in case you have a more contemporary version of the software.

For **gated**, configuration is involved. You need to explicitly exclude the vmnet1 interface from any protocol activity. If you need to run virtual machines on a host-only network on a multihomed system where **gated** is used and have problems doing so, please contact VMware technical support by submitting a support request on the VMware web site.

Potential Issues with Host-Only Networking on Linux

The following are common issues you might encounter when you are configuring a host-only network.

DHCPD on the Linux Host Does Not Work After Installing Workstation

If you were running the DHCP server program `dhcpd` on your machine before installing Workstation, it probably was configured to respond to DHCP requests from clients on any network interface present on the machine. When host-only networking is configured, an additional network interface, `vmnet1`, is marked “up” and available for use, and `dhcpd` might notice this.

In such cases, some `dhcpd` implementations abort if their configuration files do not include a subnet specification for the interface—even if `dhcpd` is not supposed to respond to messages that arrive through the interface.

The best solution is to add a line in the following format to the `dhcpd` configuration file:

```
subnet <net>.0 netmask 255.255.255.0 {}
```

<net> is the network number assigned to your host-only network—for example, 192.168.0. This line in the configuration file informs `dhcpd` about the host-only network and tells it explicitly not to respond to any DHCP requests it sees coming from it.

An alternative solution is to explicitly state the set of network interfaces that you want `dhcpd` to listen to each time you start the program. For example, if your machine has one Ethernet interface, `eth0`, each time you start `dhcpd`, list it on the command line:

```
dhcpd eth0
```

This keeps `dhcpd` from probing for all available network interfaces.

If these solutions do not work for your DHCP server program, it is probably an old DHCP server. You can try upgrading to a more current version such as the DHCP software available from the Internet Systems Consortium (ISC) web site.

DHCP and Dynamic Domain Name Service (DDNS)

Use DHCP to supply IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway. The DHCP server in Workstation does not provide a means to dynamically establish a relationship between the IP address it assigns and a client’s name (that is, to update a DNS server using DDNS).

To use names to communicate with other virtual machines you must either edit the DHCP configuration file for `vmnet1` (`/etc/vmware/vmnet1/dhcpd/dhcpd.conf`) or use IP addresses that are statically bound to a host name. Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the manual pages `dhcpd(8)` and `dhcpd.conf(8)`.

NOTE The edits to the DHCP configuration file are lost the next time you configure Workstation by running the `vmware-config.pl` file.

Set Up a Second Bridged Network Interface on a Linux Host

If you have two network adapters installed on your host computer, connected to two different networks, you might want your virtual machines on that host computer to bridge to both network adapters so the virtual machines can access either or both physical networks.

When you install Workstation on a host computer with multiple network adapters, you can configure more than one bridged network. You can also configure additional bridged networks at any time by rerunning `vmware-config.pl`.

To set up a second bridged network interface on a Linux host

- 1 On the host computer, become root (`su -`) and run the Workstation configuration program:

```
vmware-config.pl
```

- 2 If you have more than one physical network adapter, enter **yes** at the following prompt:

```
The following bridged networks have been defined:
```

```
. vmnet0 is bridged to eth0
```

```
Do you wish to configure another bridged network? (yes/no) [no]
```

If you have additional physical network adapters not yet connected to a bridged network, the prompt is repeated, showing information about all currently configured bridged networks.

- 3 When you have set up all the bridged networks you want, enter **no**.

Setting Up Two Separate Host-Only Networks

For some configurations, you might need to set up more than one host-only network on the same host computer. You might, for example, want to have two virtual machines connected to one host-only network, and at the same time have other virtual machines

connected to another host-only network so the network traffic on each network is isolated.

Or you might want to test routing between two virtual networks. Or you might want to test a virtual machine with multiple network interface cards, without using any physical network adapters.

On both Windows and Linux hosts, the first host-only network is set up automatically when you install Workstation.

Set up a Second Host-Only Network on a Windows Host

To set up a second host-only network on a Windows host

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 On the **Host Virtual Adapters** tab, click **Add**.
- 3 Choose the virtual network on which you want to use the adapter and click **OK**.
- 4 Click **OK** to close the virtual network editor.

Set up a Second Host-Only Network on a Linux Host

To set up a second host-only network on a Linux host

- 1 As root (`su -`), run the Workstation configuration program:

```
/usr/bin/vmware-config.pl
```
- 2 When you see the following prompt, enter **yes**:

Do you want to be able to use host-only networking in your virtual machines?

The wizard reports on host-only networks that you have already set up on the host or, if none is present, configures the first host-only network.
- 3 When you see the following prompt, enter **yes**:

Do you wish to configure another host-only network?

Repeat this step until you have as many host-only networks as you want, and then enter **no**.
- 4 Complete the remaining steps in the wizard. When it is finished, it restarts all services used by Workstation.
- 5 Run `ifconfig`.

At least four network interfaces appear: `eth0`, `lo`, `vmnet1`, and `vmnet2`. If the `vmnet` interfaces do not show up immediately, wait for a minute, and run the command again. These four interfaces should have different IP addresses on separate subnets.

Configuring the Host-Only Virtual Machines

Now you have two host-only interfaces (`vmnet1` and `vmnet2`). You are ready to set up your virtual machines for one of the following configurations:

- **Configuration 1** – The virtual machine is configured with one virtual network adapter, and that virtual adapter is connected to the default host-only interface (`vmnet1`). To use this configuration, see [“Set Up Using Configuration 1 or 2”](#) on page 288.
- **Configuration 2** – The virtual machine is configured with one virtual network adapter, and that virtual adapter is connected to the newly created host-only interface (`vmnet2`). To use this configuration, see [“Set Up Using Configuration 1 or 2”](#) on page 288.
- **Configuration 3** – The virtual machine is configured with two virtual network adapters. One virtual adapter is connected to the default host-only interface (`vmnet1`) and the other virtual adapter is connected to the newly created host-only interface (`vmnet2`). To use this configuration, see [“Set Up Using Configuration 3”](#) on page 289.

Set Up Using Configuration 1 or 2

To set up using configuration 1 or 2

- 1 Select the virtual machine.
It can be either powered off or powered on.
- 2 From the Workstation menu bar, choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 On the **Hardware** tab, select **Ethernet**.
- 4 In the **Network Connection** section, do one of the following:
 - To connect to the default host-only interface (`vmnet1`), select **Host-only**.
 - To connect to the newly created host-only interface, select **Custom**, and choose **vmnet2 (Host-only)** from the drop-down list on the right.

- 5 (Optional) If no network adapter is shown in the list of devices, add one, as described in [“Add Virtual Network Adapters”](#) on page 268.

Set Up Using Configuration 3

To set up using configuration 3

- 1 Select the virtual machine.
Make sure the virtual machine is powered off.
- 2 From the Workstation menu bar, choose **VM > Settings**.
The virtual machine settings editor opens.
- 3 On the **Hardware** tab, select **Ethernet**.
- 4 Connect the two adapters, as follows:
 - a Select the first network adapter in the list of devices, and in the **Network Connection** section, select **Host-only**.
This adapter is connected to the default host-only interface (vmnet1),
 - b Select the second network adapter in the list, and in the **Network Connection** section, select **Custom** and choose **vmnet2 (Host-only)** from the drop-down list.
- 5 (Optional) If no network adapter is shown in the list of devices, add one, as described in [“Add Virtual Network Adapters”](#) on page 268.

Complete Configuring the Virtual Network Adapters

To complete configuring the virtual network adapters

- 1 Power on the virtual machine and install your guest operating system.
In configurations 1 and 2, you see one network adapter. In configuration 3, you see two network adapters within the guest.
- 2 Configure the network adapters as you would physical adapters on a physical computer, giving each an IP address on the appropriate vmnet subnet.
To see what IP address a host-only network is using:
 - On Windows hosts, open a command prompt and run:
`ipconfig /all`
 - On Linux hosts, open a terminal and run:

ifconfig

Set Up Routing Between Two Host-Only Networks

If you are setting up a complex test network that uses virtual machines, you might want to have two independent host-only networks with a router between them.

There are two basic approaches. In one, the router software runs on the host computer. In the other, the router software runs in its own virtual machine. In both cases, you need two host-only interfaces.

The examples described here outline the simplest case, with one virtual machine on each of the host-only networks. For more complex configurations, you can add more virtual machines and host-only networks, as appropriate.

To set up routing between two host-only networks

- 1 Set up the connection to the first (default) host-only interface, as described in [“Set Up Using Configuration 1 or 2”](#) on page 288.
- 2 Set up the connection to the second (vmnet2) host-only interface, as described in [“Set Up Using Configuration 1 or 2”](#) on page 288.
- 3 (Optional) If you plan to run the router software on a virtual machine, set up a third virtual machine with connections to the two host only interfaces, as described in [“Set Up Using Configuration 3”](#) on page 289.

To run the router software on your host computer, skip this step.

The rest of the steps in this procedure describe how to configure the virtual machines to use static IP addresses.

- 4 Stop the vmnet DHCP server service:
 - On a Windows host, from the Workstation menu bar, choose **Edit > Virtual Network Settings > DHCP**, select the service and click **Stop**.
 - On a Linux host, open a terminal and use the following command to stop the vmnet-dhcpd service:

```
killall -TERM vmnet-dhcpd
```
- 5 Install guest operating systems in each of the virtual machines.
- 6 Install the router software, either on the host computer or in the third virtual machine, depending on the approach you are using.
- 7 Configure networking in the first two virtual machines to use addresses on the appropriate host-only network:

- On Windows hosts, open a command prompt and run `ipconfig /all` to see which IP addresses each host-only network is using.
- On Linux hosts, open a terminal and run `ifconfig` to see which IP addresses each host-only network is using.

8 Assign IP addresses by doing one of the following:

- If you are running the router on the host computer, assign default router addresses based on the addresses of the host-only adapters on the host computer.

In the first virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to `vmnet1`. In the second virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to `vmnet2`.

- If you are running the router software in a third virtual machine, set the default router addresses in the first two virtual machines based on those used by the third virtual machine.

In the first virtual machine's networking configuration, the default router address should be the IP address for the third virtual machine's network adapter connected to `vmnet1`. In the second virtual machine's networking configuration, the default router address should be the IP address for the third virtual machine's network adapter connected to `vmnet2`.

You can now be able to ping the router machine from virtual machines 1 and 2. If the router software is set up correctly, you can communicate between the first and second virtual machines.

Using Virtual Network Adapters in Promiscuous Mode on a Linux Host

Workstation does not allow the virtual network adapter to go into promiscuous mode unless the user running Workstation has permission to make that setting. This follows the standard Linux practice that only root can put a network interface into promiscuous mode.

When you install and configure Workstation, you must run the installation as root. Workstation creates the vmnet devices with root ownership and root group ownership, which means that only root has read and write permissions to the devices.

To set the virtual machine's network adapter to promiscuous mode, you must launch Workstation as root because you must have read and write access to the vmnet device. For example, if you are using bridged networking, you must have access to `/dev/vmnet0`.

To grant selected other users read and write access to the vmnet device, you can create a new group, add the appropriate users to the group and grant that group read and write access to the appropriate device. You must make these changes on the host operating system as root (`su -`). For example, you can enter the following commands:

```
chgrp <newgroup> /dev/vmnet0
chmod g+rw /dev/vmnet0
```

`<newgroup>` is the group that should have the ability to set vmnet0 to promiscuous mode.

For all users to be able to set the virtual network adapter (`/dev/vmnet0` in the example) to promiscuous mode, run the following command on the host operating system as root:

```
chmod a+rw /dev/vmnet0
```

Using NAT

NAT provides a way for virtual machines to use most client applications over almost any type of network connection available to the host. The only requirement is that the network connection must support TCP/IP.

NAT is useful when you have a limited supply of IP addresses or are connected to the network through a non-Ethernet network adapter. NAT works by translating addresses of virtual machines in a private vmnet network to that of the host machine. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request is coming from the host machine.

The host computer has a host virtual adapter on the NAT network (identical to the host virtual adapter on the host-only network). This adapter allows the host and the virtual machines to communicate with each other for such purposes as file sharing. The NAT device never forwards traffic from the host virtual adapter.

How the NAT Device Uses the vmnet8 Virtual Switch

The NAT device is connected to the vmnet8 virtual switch. Virtual machines connected to the NAT network also use the vmnet8 virtual switch.

The NAT device waits for packets coming from virtual machines on the vmnet8 virtual network. When a packet arrives, the NAT device translates the address of the virtual machine to that of the host before forwarding the packet to the external network. When data arrives from the external network for the virtual machine on the private network, the NAT device receives the data, replaces the network address with that of the virtual machine and forwards the data to the virtual machine on the virtual network. This translation occurs automatically and requires minimal configuration on the guest and the host.

DHCP on the NAT Network

To make networking configuration easy, a DHCP server is installed when you install Workstation. Virtual machines running on the network with the NAT device can dynamically obtain their IP addresses by sending out DHCP requests.

The DHCP server on the NAT network, which is also used in host-only networking configurations, dynamically allocates IP addresses in the range of <net>.128 through <net>.254, where <net> is the network number assigned to your NAT network. Workstation always uses a Class C address for NAT networks. IP addresses <net>.3 through <net>.127 can be used for static IP addresses. IP address <net>.1 is reserved for the host adapter; <net>.2 is reserved for the NAT device. For more information, see [“DHCP Conventions for Assigning IP Addresses”](#) on page 279.

In addition to the IP address, the DHCP server on the NAT network sends out configuration information that enables the virtual machine to operate. This information includes the default gateway and the DNS server. In the DHCP response, the NAT device instructs the virtual machine to use the IP address <net>.2 as the default gateway and DNS server. This causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

DNS on the NAT Network

The NAT device acts as a DNS server for the virtual machines on the NAT network. Actually, the NAT device is a DNS proxy and merely forwards DNS requests from the

virtual machines to a DNS server that is known by the host. Responses come back to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from DHCP, the virtual machines on the NAT network automatically use the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

The virtual machines in the private NAT network are not, themselves, accessible through DNS. If you want the virtual machines running on the NAT network to access each other by DNS names, you must set up a private DNS server connected to the NAT network.

External Access from the NAT Network

In general, any protocol using TCP or UDP can be used automatically by a virtual machine on the NAT network as long as the virtual machine initiates the network connection. This is true for most client applications such as Web browsing, Telnet, passive-mode FTP, and downloading streaming video. Additional protocol support has been built into the NAT device to allow FTP and ICMP echo (ping) to work transparently through the NAT.

On the external network to which the host is connected, any virtual machine on the NAT network appears to be the host itself, because its network traffic uses the host's IP address. It is able to send and receive data using TCP/IP to any machine that is accessible from the host.

Before any communication can occur, the NAT device must set up a mapping between the virtual machine's address on the private NAT network and the host's network address on the external network.

When a virtual machine initiates a network connection with another network resource, this mapping is created automatically. The operation is transparent to the user of the virtual machine on the NAT network. No additional work needs to be done.

The same cannot be said for network connections that are initiated from the external network to a virtual machine on the NAT network. When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach the virtual machine because the NAT device does not forward the request. Network connections that are initiated from outside the NAT network are not transparent.

However, it is possible to configure port forwarding manually on the NAT device so network traffic destined for a certain port can still be forwarded automatically to a virtual machine on the NAT network. See [“Advanced NAT Configuration”](#) on page 295.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network, including virtual machines and the host computer. If you are using WINS servers on your network, a virtual machine using NAT networking can access shared files and folders on the host that are known by the WINS server so long as those shared files and folders are in the same workgroup or domain.

Advanced NAT Configuration

This sections provides information for advanced users on how to configure NAT to make custom configuration settings for Windows and Linux.

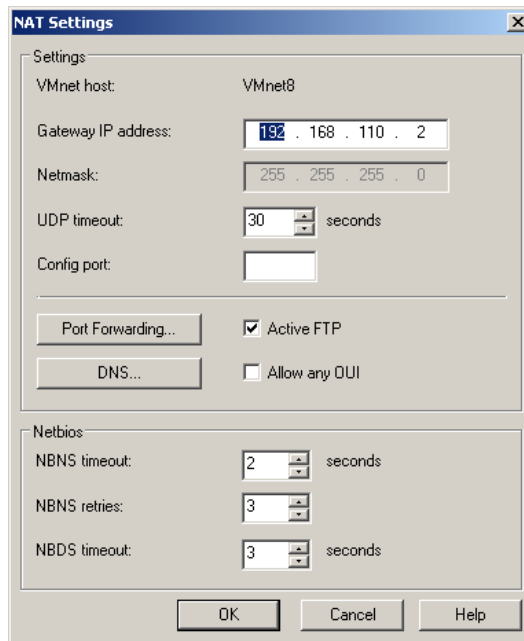
Configure NAT on a Windows Host

Use the virtual network settings editor to configure NAT on Windows host. To edit the NAT configuration file, see [“Custom NAT and DHCP Configuration on a Windows Host”](#) on page 296.

To configure NAT on a Windows host

- 1 From the Workstation menu bar, choose **Edit > Virtual Network Settings**.
- 2 Use the controls on the **NAT** tab to configure NAT:
 - Stop and start the virtual NAT device by clicking the appropriate buttons.
 - To edit NAT settings for a virtual network, choose the vmnet network from the drop-down menu and click **Edit**.

- The NAT Settings dialog box appears.



- 3 Click the appropriate button to set up or change port forwarding or to specify DNS servers the virtual NAT device should use.
- 4 Click **OK** to close the virtual network editor.

Custom NAT and DHCP Configuration on a Windows Host

If you are an advanced user on a Windows host computer, you can make custom configuration settings by editing the NAT and DHCP configuration files. If your host operating system is installed on the C drive, the configuration files for NAT and DHCP are in the following locations:

- **NAT:** C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf

For more information about this file, see [“Contents of the NAT Configuration File”](#) on page 298.

- **DHCP:** C:\Documents and Settings\All Users\Application Data\VMware\vmnetdhcp.conf

You can change many key NAT and DHCP settings using the virtual network settings editor, **Edit > Virtual Network Settings**.

NOTE If you make manual changes to the configuration files, those changes might be lost when you use the virtual network settings editor. Make backup copies of the files before changing any settings in the virtual network settings editor. You can then copy your manual changes back into the appropriate configuration files.

Specifying Connections from Ports Below 1024

When a client machine makes a TCP or UDP connection to a server, the connection comes from a particular port on the client (the source port) and connects to a particular port on the server (the destination port). For security reasons, some servers accept connections only from source ports below 1024. You might see this configuration on machines used as NFS file servers, for example.

If a virtual machine using NAT attempts to connect to a server that requires the client to use a source port below 1024, it is important that the NAT device forward the request from a port below 1024. You can specify this behavior in the `vmnetnat.conf` file.

This behavior is controlled by entries in sections headed `[privilegedUDP]` and `[privilegedTCP]`. You might need to add settings to or modify settings in either or both of these sections, depending on the kind of connection you need to make.

You can set two parameters, each of which appears on a separate line.

```
autodetect = <n>
```

The `autodetect` setting determines whether the VMware NAT device automatically attempts to map virtual machine source ports below 1024 to NAT source ports below 1024. A setting of 1 means true. A setting of 0 means false. On a Windows host, the default is 1 (true). On a Linux host, the default is 0 (false).

```
port = <n>
```

The `port` setting specifies a destination port (where `<n>` is the port on the server that accepts the connection from the client). Whenever a virtual machine connects to the specified port on any server, the NAT device attempts to make the connection from a source port below 1024. You can include one or more port settings in the `[privilegedUDP]` or `[privilegedTCP]` section or in both sections, as required for the connections you need to make. Enter each port setting on a separate line.

Configuring NAT on a Linux Host

Use the default NAT configuration file on the host to configure the NAT device. This file is located in `/etc/vmware/vmnet8/nat/nat.conf`.

The configuration file is divided into sections. Each section configures a part of the NAT device. Text surrounded by square brackets—such as `[host]`—marks the beginning of a section. In each section is a configuration parameter that can be set. The configuration parameters take the form `ip = 192.168.27.2/24`.

For an example of a NAT configuration file, see [“Sample Linux nat.conf File”](#) on page 303.

Contents of the NAT Configuration File

The NAT configuration file is located in:

- On a Windows host:
`C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf`
If you edit this file and then use the virtual network settings editor **Edit > Virtual Network Settings**. However, your edits might be lost.
- On a Linux host:
`/etc/vmware/vmnet8/nat/nat.conf`

The NAT configuration file contains the following sections.

The `[host]` Section

`ip`

The IP address that the NAT device should use. It can be followed by a slash and the number of bits in the subnet.

`netmask`

The subnet mask to use for the NAT network. DHCP addresses are allocated from this range of addresses.

`configport`

A port that can be used to access status information about the NAT device.

`device`

The vmnet device to use. Windows devices are of the form `vmnet<x>` where `<x>` is the number of the vmnet. Linux devices are of the form `/dev/vmnet<x>`.

`activeFTP`

Flag to indicate if active FTP is to be allowed. Active FTP allows incoming connections to be opened by the remote FTP server. Turning this off means that only passive mode FTP works. Set this flag to `0` to turn it off.

The [udp] Section

timeout

Number of seconds to keep the UDP mapping for the NAT network.

The [dns] Section

This section is for Windows hosts only. Linux does not use this section.

policy

Policy to use for DNS forwarding. Accepted values include:

- **order** – Send one DNS request at a time in order of the name servers.
- **rotate** – Send one DNS request at a time and rotate through the DNS servers.
- **burst** – Send to three servers and wait for the first one to respond.

timeout

Time in seconds before retrying a DNS request.

retries

Number of retries before the NAT device gives up on a DNS request.

autodetect

Flag to indicate whether the NAT device should detect the DNS servers available to the host.

nameserver1

IP address of a DNS server to use.

nameserver2

IP address of a DNS server to use.

nameserver3

IP address of a DNS server to use.

If autodetect is on and some name servers are specified, the DNS servers specified in `nameserver1`, `nameserver2` and `nameserver3` are added before the list of detected DNS servers.

The [netbios] Section

This section applies to Windows hosts only. Linux does not use this section.

nbnsTimeout = 2

Timeout, in seconds, for NBNS queries.

```
nbnsRetries = 3
```

Number of retries for each NBNS query.

```
nbdsTimeout = 3
```

Timeout, in seconds, for NBDS queries.

The [incomingtcp] Section

Use this section to configure TCP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section:

```
8887 = 192.168.27.128:21
```

This example creates a mapping from port 8887 on the host to the IP address 192.168.27.128 and port 21. When this mapping is set and an external machine connects to the host at port 8887, the network packets are forwarded to port 21 (the standard port for FTP) on the virtual machine with IP address 192.168.27.128.

The [incomingudp] Section

Use this section to configure UDP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section. It illustrates a way to forward X server traffic from the host port 6000 to the virtual machine's port 6001:

```
6000 = 192.168.27.128:6001
```

This example creates a mapping from port 6000 on the host to the IP address 192.168.27.128 and port 6001. When this mapping is set and an external machine connects to the host at port 6000, the network packets are forwarded to port 6001 on the virtual machine with IP address 192.168.27.128.

Considerations for Using NAT

Following are the considerations to take into account when you use NAT:

- NAT causes some performance loss.

Because NAT requires that every packet sent to and received from a virtual machine must be in the NAT network, there is an unavoidable performance penalty.

- NAT is not perfectly transparent.

It does not normally allow connections to be initiated from outside the network, although you can set up server connections by manually configuring the NAT

device. The practical result is that some TCP and UDP protocols that require a connection be initiated from the server machine—some peer to peer applications, for example—do not work automatically, and some might not work at all.

- NAT provides some firewall protection.

A standard NAT configuration provides basic-level firewall protection because the NAT device can initiate connections from the private NAT network, but devices on the external network cannot normally initiate connections to the private NAT network.

Using NAT with NetLogon

When using NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can use NetLogon to log on to a Windows domain from the virtual machine. You can then access file shares known by the WINS server in the domain.

To use NetLogon, you need to know how WINS servers and Windows domain controllers work. This section explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you set up a physical computer on one LAN that is using a domain controller on another LAN.

To log on to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. You can connect the virtual machine to a WINS server in two ways:

- Connect to the WINS server provided by the DHCP server used on the NAT network, if the WINS server is already set up on the host.
- To connect from the virtual machine to a WINS server not set up on the host, you can manually enter the IP address of the WINS server.

This section provides instructions for both strategies.

Use NAT to Connect to an Existing WINS Server Set Up on the Host

In order to use this method, a WINS server in the same workgroup or domain must be set up on the host. These steps use Windows 2000, Windows XP, or Windows 2003 Server as a guide. The process is similar for Windows NT, Windows Me, and Windows 9x guests. For Windows Vista, the first couple of steps are different, as noted in the specific steps below.

To use NAT to connect to an existing WINS server set up on the host

- 1 In the virtual machine, right-click **My Network Places** and choose **Properties**.
For Windows Vista, open the Network and Sharing Center, and click the **View Status** link for the connection that uses the desired virtual network adapter.
- 2 In the Network Connections window, right-click the virtual network adapter and choose **Properties**.
For Windows Vista, in the Connection Status window, click **Properties** and click **Continue** when prompted for permission.
- 3 In the Properties dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.
- 4 In the TCP/IP Properties dialog box, click **Advanced**.
- 5 On the **WINS** tab, under NetBIOS setting, select **Use NetBIOS setting from DHCP Server**.
- 6 Click **OK** twice and click **Close**.

Enter the IP Address of a WINS Server Manually

Use this method to connect to a WINS server in the same workgroup or domain that is not already set up on the host.

To enter the IP address of a WINS server manually

- 1 In the virtual machine, right-click **My Network Places** and choose **Properties**.
For Windows Vista, open the Network and Sharing Center, and click the **View Status** link for the connection that uses the virtual network adapter.
- 2 In the Network Connections window, right-click the virtual network adapter and choose **Properties**.
For Windows Vista, in the Connection Status window, click **Properties** and click **Continue** when prompted for permission.
- 3 In the Properties dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.
- 4 In the TCP/IP Properties dialog box, click **Advanced**.
- 5 On the **WINS** tab, click **Add**.
- 6 In the TCP/IP WINS Server dialog box, enter the IP address for the WINS server in the WINS server field and click **OK**.
The IP address of the WINS server appears in the WINS addresses list on the WINS tab.

- 7 Repeat [Step 5](#) and [Step 6](#) for each WINS server to which you want to connect from this virtual machine.
- 8 Click **OK** twice and click **Close**.

Now that the virtual machine has an IP address for a WINS server, you can use NetLogon in the virtual machine to log on to a domain and access shares in that domain. However, your access is limited to shares of virtual machines that are on the same NAT network or are bridged on the same domain.

For example, if the WINS server covers a domain with a domain controller, it is possible to access that domain controller from the virtual machine and add the virtual machine to the domain. You need to know the user ID and password of the Administrator user on the domain controller.

Sample Linux nat.conf File

```
# Linux NAT configuration file

[host]

# NAT gateway address
ip = 192.168.237.2/24
hostMAC = 00:50:56:C0:00:08

# enable configuration; disabled by default for security reasons
#configport = 33445

# vmnet device if not specified on command line
device = vmnet8

# Allow PORT/EPRT FTP commands (they need incoming TCP stream...)
activeFTP = 1

# Allows the source to have any OUI. Turn this one if you change the OUI
# in the MAC address of your virtual machines.
#allowAnyOUI = 1

[udp]
# Timeout in seconds, 0 = no timeout, default = 60; real value might
# be up to 100% longer
timeout = 30

[dns]
# This section applies only to Windows.
#
# Policy to use for DNS forwarding. Accepted values include order,
# rotate, burst.
#
```

```

# order: send one DNS request at a time in order of the name servers
# rotate: send one DNS request at a time, rotate through the DNS servers
# burst: send to three servers and wait for the first one to respond
policy = order;

# Timeout in seconds before retrying DNS request.
timeout = 2

# Retries before giving up on DNS request
retries = 3

# Automatically detect the DNS servers (not supported in Windows NT)
autodetect = 1

# List of DNS servers to use. Up to three may be specified
#nameserver1 = 208.23.14.2
#nameserver2 = 63.93.12.3
#nameserver3 = 208.23.14.4

[netbios]
# This section applies only to Windows.

# Timeout for NBNS queries.
nbnsTimeout = 2

# Number of retries for each NBNS query.
nbnsRetries = 3

# Timeout for NBDS queries.
nbdsTimeout = 3

[incomingtcp]
# Use these with care – anyone can enter into your virtual machine through
# these...

# FTP (both active and passive FTP is always enabled)
# ftp localhost 8887
#8887 = 192.168.27.128:21

# WEB (make sure that if you are using named webhosting, names point to
# your host, not to guest... And if you are forwarding port other
# than 80 make sure that your server copes with mismatched port
# number in Host: header)
# lynx http://localhost:8888
#8888 = 192.168.27.128:80

# SSH
# ssh -p 8889 root@localhost
#8889 = 192.168.27.128:22

```



```
[incomingudp]
# UDP port forwarding example
#6000 = 192.168.27.128:6001
```

Using Samba with Workstation

If you have Samba running on your Linux host, you can configure Samba so that it works with Workstation, as described in this section.

Modify your Samba configuration so that it includes the IP subnet used by the Workstation virtual network adapter, `vmnet1`. To determine which subnet is being used by `vmnet1`, run:

```
/sbin/ifconfig vmnet1
```

Make sure the Samba password file includes entries for all users of the virtual machine who will access the host's file system. The user names and passwords in the Samba password file must match those used for logging on to the guest operating system.

Add Users to the Samba Password File

You can add user names and passwords to the Samba password file at any time from a terminal window on your Linux host computer.

To add users to the Samba password file

- 1 Log on to the root account:

```
su
```
- 2 Run the Samba password command:

```
smbpasswd -a <username>
```

`<username>` is the user name to add.
- 3 Follow the instructions on the screen.
- 4 Log out of the root account:

```
exit
```

Using a Samba Server for Bridged and Host-Only Networks

To use your Samba server for both host-only and bridged networking, you must modify one parameter in the `smb.conf` file. You can define the `interface` parameter so your Samba server serves multiple interfaces. An example of this is:

```
interface = eth0 vmnet1
```

This example tells the Samba server to listen to and use both the eth0 and vmnet1 interfaces, which are the interfaces used by bridged and host-only networking, respectively.

Use Samba Without Network Access

To use Samba without network access

- 1 Open the configuration file:
`/etc/samba/smb.conf`
- 2 Add the following line to the configuration file and save the changes.
`interfaces = vmnet*`
- 3 Restart Samba.

Configuring Video and Sound

17

The following sections provide information on configuring the video display and sound for VMware Workstation. This chapter includes the following topics:

- [“Setting Screen Color Depth”](#) on page 307
- [“Support for Direct3D Graphics”](#) on page 308
- [“Configuring Sound”](#) on page 310

Setting Screen Color Depth

The number of screen colors available in the guest operating system depends on the screen color setting of the host operating system.

Virtual machines support:

- 16-color (VGA) mode
- 8-bit pseudocolor
- 16 bits per pixel (16 significant bits per pixel)
- 32 bits per pixel (24 significant bits per pixel)

If the host is in 15-bit color mode, the guest operating system’s color setting controls offer 15-bit mode in place of 16-bit mode.

If the host is in 24-bit color mode, the guest operating system’s color setting controls offer 24-bit mode in place of 32-bit mode.

If you run a guest operating system set for a greater number of colors than your host operating system is using, you can encounter various problems. In some cases, for example, the colors in the guest are not correct. In others, the guest operating system is not able to use a graphical interface.

You can try either of the following solutions:

- Increase the number of colors available on the host, as described in [“Changing Screen Color Depth on the Host”](#) on page 308.
- Decrease the number of colors used in the guest, as described in [“Changing Screen Color Depth in the Virtual Machine”](#) on page 308.

For best performance, use the same number of colors in the guest and on the host.

Changing Screen Color Depth on the Host

If you choose to change the color settings on your host operating system, shut down all guest operating systems, power off the virtual machines, and close Workstation.

Follow standard procedures for changing the color settings on your host operating system, and then restart Workstation and the virtual machines.

Changing Screen Color Depth in the Virtual Machine

If you choose to change the color settings in the guest operating system, the approach you take depends on the guest operating system.

Follow the normal process for changing screen colors in your guest operating system:

- In a Windows guest, the Display Properties control panel offers only those settings that are supported.
- In a Linux or FreeBSD guest, you must change the color depth before you start the X server or restart the X server after making the changes.

Support for Direct3D Graphics

To take advantage of the 3-D capabilities of Workstation, the virtual machine must be running the version of VMware Tools included with Workstation 6.5 or higher. For example, you do not need to upgrade a Workstation 6.0 virtual machine to Workstation 6.5, but you do need to upgrade the VMware Tools running inside it. If you move the virtual machine and want to use the 3-D capabilities, be sure you have the correct version of VMware Tools installed.

Accelerated 3-D Restrictions

Support for applications that use DirectX 9 accelerated graphics applies only to Windows XP guests, on hosts running Windows 2000, Windows XP, Windows Vista, or Linux.

This feature currently has the following restrictions:

- Workstation now offers support for DirectX games and applications whose versions are up to DirectX 9.
- Support for 3-D applications is not optimized for performance.
- OpenGL applications run in software emulation mode.

Enabling Accelerated 3-D

By default, Direct3D technology is enabled for Workstation 6 and later virtual machines. You must prepare the host first, the virtual machine second, and the guest operating system last.

To enable a host for accelerated 3-D

- 1 With regards to hardware, the host must have a video card capable of running accelerated OpenGL 2.0.

If you are unsure, check with your hardware manufacturer.

- 2 With regards to software, upgrade the host's video drivers to the latest version available:

- AMD drivers are available at:

ati.amd.com/support/driver.html

- NVIDIA drivers are available at:

www.nvidia.com/content/drivers/drivers.asp

Be sure to follow the video card manufacturer's instructions carefully. This feature is not supported on Linux hosts with drivers below version 8.02.

- 3 If you are using a Windows XP host, make sure hardware acceleration is turned up in the display properties:
 - a Right-click the desktop and choose **Properties>Settings>Advanced>Troubleshoot**.
 - b Move the **Hardware Acceleration** slider all the way to the **Full** position.
- 4 If you are using Linux, test your Linux host for compatibility:
 - a To verify that direct rendering is enabled, run:


```
glxinfo | grep direct
```
 - b To ensure that 3-D applications work on your host, run:

glxgears

After your host is configured, configure a virtual machine for accelerated 3-D.

To enable a virtual machine for accelerated 3-D

- 1 Choose a virtual machine with a Windows XP guest operating system.
Do not enable Direct3D on a virtual machine that is powered on or suspended.
- 2 Make sure the virtual machine is powered off.
- 3 Select the virtual machine and choose **VM > Settings > Hardware > Display**.
- 4 In the **Monitors** section, if the virtual machine is set to use more than one monitor, set it to use only one monitor.
- 5 In the **3D Graphics** section, make sure the check box is selected and click **OK**.

To enable the guest operating system for accelerated 3-D

- 1 Power on the virtual machine.
- 2 Install VMware Tools.
For instructions, see “[Installing VMware Tools](#)” on page 105.
- 3 Install DirectX 9.0c End User Runtime.
This download is available from Microsoft at:
www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=2
- 4 Install and run your 3-D applications.

Configuring Sound

Workstation provides a sound device compatible with the Sound Blaster AudioPCI and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Linux guest operating systems. The Workstation sound device is enabled by default.

Sound support includes PCM (pulse code modulation) output and input. For example, you can play .wav files, MP3 audio, and Real Media audio. MIDI output from Windows guests is supported through the Windows software synthesizer. MIDI input is not supported, and no MIDI support is available for Linux guests.

Windows 2000, Windows XP, and most recent Linux distributions automatically detect the sound device and install appropriate drivers for it.

For Windows Vista, when you install VMware Tools in a 64-bit Windows Vista guest operating system, a sound driver is installed. For 32-bit Windows Vista guests and Windows 2003 Server guests, you need to use Windows Update to install a 32-bit driver.

Installing Sound Drivers in Windows 9x and NT Guests

Windows 95, Windows 98, Windows 98SE, and Windows NT 4.0 do not have drivers for the Sound Blaster AudioPCI adapter. To use sound in these guest operating systems, download the driver from the Creative Labs Web site (www.creative.com) and install it in the guest operating system.

Creative Labs has a number of Web sites serving various regions of the world. The adapter name varies, depending on the region, but usually includes PCI 128.

BETA

BETA

Connecting Devices

This chapter describes how to use various devices with a virtual machine. This chapter includes the following topics:

- [“Using Parallel Ports”](#) on page 313
- [“Using Serial Ports”](#) on page 318
- [“Configuring Keyboard Features”](#) on page 324
- [“Using USB Devices in a Virtual Machine”](#) on page 335
- [“Use Smart Cards with Virtual Machines”](#) on page 342
- [“Support for Generic SCSI Devices”](#) on page 343
- [“Use Two-Way Virtual Symmetric Multiprocessing”](#) on page 348

Using Parallel Ports

Parallel ports are used by a variety of devices, including printers, scanners, dongles, and disk drives.

Currently, Workstation provides only partial emulation of PS/2 hardware. Interrupts requested by a device connected to the physical port are not passed to the virtual machine. Also, the guest operating system cannot use DMA (direct memory access) to move data to or from the port. For this reason, not all devices that attach to the parallel port are guaranteed to work correctly.

Add a Virtual Parallel Port to a Virtual Machine

If the virtual machine is configured with a parallel port, most guest operating systems detect it at installation time and install the required drivers. Some operating systems,

including Linux, Windows NT, and Windows 2000, automatically detect the ports at boot time. Others, like Windows 95 and Windows 98, do not.

To add a virtual parallel port to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the New Hardware wizard.
- 5 Select **Parallel Port** and click **Next**.
- 6 Specify which option you want to use for the parallel port:
 - If you select **Use physical parallel port**, click **Next** and choose the port from the drop-down list.
 - If you select **Output file**, click **Next** and enter the path and filename or browse to the location of the file.
- 7 Under **Device status**, if you do not want the parallel port to connect at power on, clear the check box.
- 8 Click **Finish**.

In a Windows 95 or Windows 98 guest, after you add the port, run the guest operating system's Add New Hardware wizard (choose **Start > Settings > Control Panel > Add New Hardware**). Let Windows detect the new device.

Drivers for Iomega Zip Drives on Windows 95 and 98 Guests

On Windows 95 or Windows 98, use of older drivers for the Iomega Zip drive might cause the guest operating system to lock up intermittently at boot time or during installation of the guest operating system. The newest Iomega drivers work reliably in VMware tests. To get the drivers, go to the Iomega Web site and click on **Support & Downloads**.

Configuring a Parallel Port on a Linux Host

For a parallel port to work properly in a guest, it must first be configured properly on the host. Most issues with parallel ports are caused by mistakes in the host configuration. The topics that follow provides troubleshooting procedures for checking the version of the Linux kernel, device access permissions, and required modules.

Linux kernels in the 2.4.x and 2.6.x series also use a special arbitrator for access to the parallel port hardware. If the parallel port is in use by the host, the virtual machine cannot use it. If a virtual machine is using the parallel port, the host and any users accessing the host are denied access to the device. You must use the **VM > Removable Devices** to disconnect the parallel port from the virtual machine if you want to access the device from the host.

Configure Parallel Ports for Linux 2.2.x Kernels

The 2.2.x kernels that support parallel ports use the `parport`, `parport_pc`, and `vmppuser` modules. Workstation requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module. That is, it must be set to “m”. Workstation is unable to use parallel port devices if `CONFIG_PARPORT_PC` is built directly (compiled) into the kernel. This limitation exists because `CONFIG_PARPORT_PC` does not correctly export its symbols.

The `vmppuser` module supplied by Workstation gives virtual machines user-level access to the parallel port.

To configure parallel ports for Linux 2.2.x kernels

- 1 Determine whether the `parport`, `parport_pc`, and `vmppuser` modules are installed and running on your system by running the `lsmod` command as the root user.

These three modules are included in the listing of running modules. You can also look at the `/proc/modules` file for the list.

- 2 To load the proper modules, run this command:

```
insmod <modulename>
```

- 3 If none of the listed parallel port modules is loaded, use this command:

```
insmod parport_pc
```

This command inserts the three modules needed for a parallel port.

If you continue to see problems, it is possible that the `lp` module is running. If it is, the virtual machine cannot use the parallel port correctly.

- 4 If the `lp` module is loaded, run this command as the root user to remove it:

```
rmmod lp
```

- 5 Verify that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a hash character (#) at the beginning of the line.

The name of the configuration file depends on the Linux distribution. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

- 6 To ensure that the proper modules for the parallel port are loaded at boot time, add this line to the `/etc/modules.conf` or `/etc/conf.modules` file:

```
alias parport_lowlevel parport_pc
```

Configure Parallel Ports for Linux 2.4.x Kernels

The 2.4.x kernels that support parallel ports use the `parport`, `parport_pc`, and `ppdev` modules. Workstation requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module. That is, it must be set to “m”. Support for user-space parallel device drivers (`CONFIG_PPDEV`) must also be enabled.

To configure parallel ports for Linux 2.4.x kernels

- 1 Determine whether the `parport`, `parport_pc`, and `ppdev` modules are installed and loaded on your system by running the `lsmod` command as the root user.

These three modules are included in the listing of loaded modules. You can also look at the `/proc/modules` file for the list.

- 2 To load the proper modules, run this command:

```
insmod <modulename>
```

- 3 If none of the listed parallel port modules is loaded, use this command:

```
insmod parport_pc
```

This command inserts the `parport` and `parport_pc` modules needed for a parallel port.

- 4 Use this command to load the `ppdev` module:

```
insmod ppdev
```

If you continue to see problems, it is possible that the `lp` module is loaded. If it is, the virtual machine cannot use the parallel port correctly.

- 5 If the `lp` module is loaded, run this command as the root user to remove it:

```
rmmod lp
```

- 6 Verify that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a hash character (#) at the beginning of the line.

The name of the configuration file depends on the Linux distribution you are using. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

- 7 To ensure that the proper modules for the parallel port are loaded at boot time, add this line to the `/etc/modules.conf` or `/etc/conf.modules` file:

```
alias parport_lowlevel parport_pc
```

Configure Parallel Ports for Linux 2.6.x Kernels

The 2.6.x kernels that support parallel ports use the `modprobe <modulename>` and `modprobe parport_pc` modules. Workstation requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module. That is, it must be set to “m”.

To configure parallel ports for Linux 2.6.x kernels

- 1 Determine whether the `modprobe <modulename>` and `modprobe parport_pc` modules are installed and loaded on your system by running the `lsmod` command as the root user.

You can also look at the `/proc/modules` file for the list.

With 2.6.x, loading `parport_pc` does not load all modules.

- 2 If none of the listed parallel port modules is loaded, use this command:

```
modprobe parport_pc && modprobe ppdev
```

This command inserts the modules needed for a parallel port.

If you continue to see problems, it is possible that the `lp` module is loaded. If it is, the virtual machine cannot use the parallel port correctly.

- 3 If the `lp` module is loaded, run this command as the root user to remove it:

```
rmmod lp
```

- 4 Verify that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a hash character (`#`) at the beginning of the line.

The name of the configuration file depends on the Linux distribution you are using. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

- 5 To ensure that the proper modules for the parallel port are loaded at boot time, add this line to the `/etc/modules.conf` or `/etc/conf.modules` file:

```
alias parport_lowlevel parport_pc
```

Configure Device Permissions for Parallel Ports

Some Linux distributions by default do not grant the virtual machine access to the `lp` and `parport` devices. You must add the VMware user to the group that has permission to access these devices.

To configure device permissions for parallel ports

- 1 Run the following command to determine the owner and group for the device:

```
ls -la /dev/parport0
```

The third and fourth columns of the output show the owner and group, respectively. In most cases, the owner of the device is `root` and the associated group is `lp`.

- 2 To add the user to the device group, become the root user and open the `/etc/group` file with a text editor.
- 3 On the line starting with `lp`, which defines the `lp` group, add the Workstation user's user name.

The following line provides an example for a user whose user name is `userj`.

```
lp::7:daemon,lp,userj
```

The next time the user logs on to the host, the changes take effect.

Using Serial Ports

A Workstation virtual machine can use up to four virtual serial ports. The virtual serial ports can be configured in several ways:

- Connect a virtual serial port to a physical serial port on the host computer.
- Connect a virtual serial port to a file on the host computer.
- Make a direct connection between two virtual machines or between a virtual machine and an application running on the host computer.

You can also select whether to connect the virtual serial port when you power on the virtual machine.

Add a Virtual Serial Port to a Virtual Machine

You can set up a virtual serial port to use a physical serial port on the host if you want to use a device such as an external modem or hand-held device in a virtual machine.

You can also set up a virtual serial port to send its output to a file on the host. This setup is useful if you want to capture the data a program running in the virtual machine sends to the virtual serial port.

To add a virtual serial port to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
- 5 Select **Serial Port** and click **Next**.
- 6 Specify which option you want to use for the serial port:
 - If you select **Use physical serial port on the host**, click **Next** and choose the port on the host computer that you want to use for this serial connection.
 - If you select **Output file**, click **Next** and enter the path and filename or browse to the location of the file.
- 7 In the **Device status** section, if you do not want the serial port to connect at power on, clear the check box.
- 8 Click **Finish** to return to the virtual machine settings editor.
- 9 (Optional) On the **Hardware** tab, to configure this serial port to use polled mode, select **Yield CPU on poll**.

This option is of interest to developers who are using debugging tools that communicate over a serial connection. If the serial port in the guest is being used in polled mode rather than interrupt mode, you might notice performance issues. This option forces the virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

Connect an Application on the Host to a Virtual Machine

You can set up the virtual serial port in a virtual machine to connect to an application on the host. This setup is useful if you want to use an application on the host to capture debugging information sent from the virtual machine's serial port.

To connect an application on the host to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.

- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
- 5 Select **Serial Port** and click **Next**.
- 6 On the Serial Port Type page, select **Output to Named Pipe** and click **Next**.
- 7 Depending on whether you are using a Linux host or a Windows host, do one of the following:
 - For a Windows host, on the Specify Named Pipe page, specify the pipe name.
The pipe name must follow the form `\\.\pipe\<namedpipe>`. That is, it must begin with `\\.\pipe\`.
 - For a Linux host, in the **Path** field, enter `/tmp/<socket>` or another UNIX socket name.
- 8 Select **This end is the server** or **This end is the client**.
Select **This end is the server** if you plan to start this end of the connection first.
- 9 Select **The other end is an application**.
- 10 Under **Device status**, if you do not want the serial port to connect at power on, clear the check box.
- 11 Click **Finish** to return to the virtual machine settings editor.
- 12 (Optional) On the **Hardware** tab, to configure this serial port to use polled mode, select **Yield CPU on poll**.

This option is of interest to developers who are using debugging tools that communicate over a serial connection. If the serial port in the guest is being used in polled mode rather than interrupt mode, you might notice performance issues. This option forces the virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.
- 13 On the host, configure the application that communicates with the virtual machine to use the same pipe name (for a Windows host) or the same UNIX socket name (for a Linux host).

Use a Serial Port Connection Between Two Virtual Machines

You can set up the virtual serial ports in two virtual machines to connect to each other. This is useful if you want to use an application in one virtual machine (the client) to capture debugging information sent from the other (the server) virtual machine's serial port.

The following procedures describe how to set up the server and the client for connecting to each other by two virtual serial ports.

To use a serial port connection between two virtual machines

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 Click **Add** to start the Add Hardware wizard.
- 5 Select **Serial Port** and click **Next**.
- 6 On the Serial Port Type page, select **Output to Named Pipe** and click **Next**.
- 7 Depending on whether you are using a Linux host or a Windows host, do one of the following:
 - For a Windows host, on the Specify Named Pipe page, specify the pipe name. The pipe name must follow the form `\\.\pipe\<namedpipe>`. That is, it must begin with `\\.\pipe\`.
 - For a Linux host, in the **Path** field, enter `/tmp/<socket>` or another UNIX socket name.
- 8 Select **This end is the server**.
- 9 Select **The other end is a virtual machine**.
- 10 Make sure the **Connect at power on** check box is selected if desired.
- 11 Click **Finish** to return to the virtual machine settings editor.
- 12 (Optional) On the **Hardware** tab, to configure this serial port to use polled mode, select **Yield CPU on poll**.

This option is of interest to developers who are using debugging tools that communicate over a serial connection. If the serial port in the guest is being used in polled mode rather than interrupt mode, you might notice performance issues. This option forces the virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

- 13 Power on the virtual machine.
- 14 Repeat [Step 1](#) through [Step 13](#) for the second virtual machine, but at [Step 8](#) select **This end is the client**.

Change the Input Speed of the Serial Connection

This option increases the speed of a serial connection over a pipe to a virtual machine. In principle, there is no limit on the output speed, which is the speed at which the virtual machine sends data through the virtual serial port. In practice, the output speed depends on how fast the application at the other end of the pipe reads data inbound to it.

To change the input speed of the serial connection

- 1 Use the guest operating system to configure the serial port for the highest setting supported by the application you are running in the virtual machine.
- 2 Power off the virtual machine and close the Workstation window.
- 3 Use a text editor to add the following line to your virtual machine's configuration (.vmx) file:

```
serial<n>.pipe.charTimePercent = "<x>"
```

<n> is the number of the serial port, starting from 0. So the first serial port is serial0.

<x> is a positive integer that specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the guest. For example, a setting of 200 forces the port to take twice as long per character, or send data at half the default speed. A setting of 50 forces the port to take only half as long per character, or send data at twice the default speed.

Assuming that the serial port speed is set appropriately in the guest operating system, experiment with this setting. Start with a value of 100 and gradually decrease it until you find the highest speed at which your connection works reliably.

Debugging over a Virtual Serial Port

Using virtual machines, you can debug kernel code on one system without the need for two physical computers, a modem, or a serial cable. You can use Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) to debug kernel code in a virtual machine over a virtual serial port.

You can Download Debugging Tools for Windows from the WHDC (Windows Hardware Developer Central) Web site.

Debug an Application in a Virtual Machine from a Windows Host

In this setup, you have kernel code to debug in a virtual machine (called the target virtual machine) and are running Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) on a Windows host.

Before you begin, on the host, make sure you have a recent version of Debugging Tools for Windows, which supports debugging over a pipe. You need version 5.0.18.0 or higher.

To debug an application in a virtual machine from a Windows host

- 1 Prepare the target virtual machine as described in [“Connect an Application on the Host to a Virtual Machine”](#) on page 319.

Make sure you configure the virtual machine’s virtual serial port as follows:

- a Select **This end is the server**.
- b Under **I/O Mode**, select the **Yield CPU on poll** check box because the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode.

- 2 Power on the virtual machine.
- 3 Use the **VM > Removable Devices** menu to make sure the serial port is connected.

On that menu, if **Serial<n>** is not reported as `\\.\pipe\<namedpipe>`, choose the virtual serial port and click **Connect**.

- 4 On the host, open a command prompt window and do one of the following:

- If you are using WinDbg, type the following:
`windbg -k com:port=\\.\pipe\<namedpipe>,pipe`
- If you are using KD, type the following:
`kd -k com:port=\\.\pipe\<namedpipe>,pipe`

- 5 Press Enter to start debugging.

Debug an Application in a Virtual Machine from Another Virtual Machine

This setup is useful if you use Workstation on a Linux host. In this situation, you have kernel code to debug in the target virtual machine and are running Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) in the debugger virtual machine on the same host.

Before you begin, download and install WinDbg or KD in the Windows guest that you plan to use as the debugger virtual machine.

To debug an application from another virtual machine

- 1 Prepare the target virtual machine by using the appropriate platform-specific procedure for the server virtual machine.

See [“Use a Serial Port Connection Between Two Virtual Machines”](#) on page 320.

On Windows hosts, under **I/O Mode**, select the **Yield CPU on poll** check box because the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode.

- 2 Follow the steps for the client virtual machine in [“Use a Serial Port Connection Between Two Virtual Machines”](#) on page 320.
- 3 Power on both virtual machines.
- 4 Use the **VM > Removable Devices** menu to make sure the serial port is connected.
If the serial port is not connected, choose the virtual serial port and click **Connect**.
- 5 In the debugger virtual machine, start debugging with WinDbg or KD.

Configuring Keyboard Features

You can change which key combinations you use for hot-key sequences in Workstation and which language to use for the keyboard that VNC clients use. In addition, you can configure platform-specific keyboard features for Windows and Linux hosts.

Use the Enhanced Virtual Keyboard for Windows Hosts

This feature provides better handling of international keyboards and keyboards with extra keys. It also offers security improvements because it processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that is not already at a lower layer. This feature is currently available for all 32-bit Windows guests except Windows Vista guests.

If you use this feature, when you press Ctrl+Alt+Delete, the guest system only, rather than both guest and host, acts on the command.

Before you begin, if you just installed or upgraded to Workstation 6.x and have not yet restarted your computer, do so.

To use the enhanced virtual keyboard for Windows hosts

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.

- 4 Click the **Options** tab, and select **General**.
- 5 To enable or disable the setting, use the **Use enhanced virtual keyboard** check box and click **OK**.

Hot Keys for Virtual Machines

Hot keys let you specify the key combination that is used with hot-key sequences for virtual machines. For example, you can require that all hot-key sequences use Ctrl+Shift+Alt.

Configuring hot keys is useful if you want to prevent certain key combinations (such as Ctrl+Alt+Del) from being intercepted by Workstation instead of being sent to the guest operating system. Use hot-key sequences to:

- Switch between virtual machines
- Enter and leave full screen mode
- Ungrab input
- Send Ctrl+Alt+Del to the virtual machine only (not to the host machine)
- Send commands to the virtual machine only (not to the host machine)

Because Ctrl+Alt tells Workstation to release (ungrab) mouse and keyboard input, combinations that include Ctrl+Alt are not passed to the guest operating system. If you need to use such a combination, press Ctrl+Alt+Space, release Space without releasing Ctrl and Alt, and press the third key of the key combination you want to send to the guest.

The default settings for hot keys are listed in the preferences editor (choose **Edit > Preferences > Hot Keys**). Use the preferences editor to change them.

Specify a Language Keyboard Map for VNC Clients

If you set a virtual machine to act as a VNC server, you can specify which language you want to use for the keyboard that VNC clients use. By default, the US101 keyboard map (U.S. English) is used.

Before you begin, determine the location of the keymap file you want to use. Default keymap files are included in the Workstation installation directory:

- On Windows hosts, this directory is in C:\Documents and Settings\All Users\Application Data\VMware\vnckeymap.
- On Linux hosts, this directory is in /usr/lib/vmware/vnckeymap.

If the keymap file you want to use is in another location, determine the path to the file.

To specify a language keyboard map for VNC clients

- 1 Set the virtual machine to act as a VNC server.
See [“Configure a Virtual Machine as a VNC Server”](#) on page 167.
- 2 Use a text editor to open the configuration file (.vmx file) for the virtual machine and add the following lines:

- **RemoteDisplay.vnc.enabled = "TRUE"**

- **RemoteDisplay.vnc.port = "<port number>"**

where <port number> is the port number you want to use.

- 3 Add one of the following properties to the configuration file:

- To use the default keymap file included in the Workstation installation directory, set the following property:

RemoteDisplay.vnc.keyMap = "<xx>"

where <xx> is the code for the language you want to use, such as jp for Japanese. Following is a list of language codes:

de: German

de-ch: German (Switzerland)

es: Spanish

fi: Finnish

fr: French

fr-be: French (Belgium)

fr-ch: French (Switzerland)

is: Icelandic

it: Italian

jp: Japanese

nl-be: Dutch (Belgium)

no: Norwegian

pt: Polish

uk: UK English

us: US English

- To use a keyboard map file in another location, set the following property to an absolute file path:

RemoteDisplay.vnc.keyMapFile

- 4 Start the virtual machine and connect to it from a VNC client.

See [“Use a VNC Client to Connect to a Virtual Machine”](#) on page 168.

Keyboard Mapping on a Linux Host

This topic addresses the following issues and provides additional details on keyboard mapping in Linux:

- The keyboard works when you run a virtual machine locally but not when you run the same virtual machine with a remote X server.
- Some of the keys on the keyboard do not work correctly in a virtual machine.
- Some language-specific keyboards do not appear to be supported by Workstation.

Configure Keyboard Mapping for a Remote X Server

Sometimes the keyboard works correctly with a local X server but not when you run the same virtual machine with a remote X server. You need to set additional properties in the configuration (.vmx) file.

Before you begin, verify that the remote X server is an XFree86 server running on a PC.

If the keyboard does not work correctly on an XFree86 server running locally, report the problem to VMware technical support.

For local X servers, Workstation maps X key codes to PC scan codes to correctly identify a key. Workstation uses this key code mapping only for local X servers because it cannot tell whether a remote X server is running on a PC or on some other kind of computer. In this case, you can set a property to tell Workstation to use key code mapping. For a description of key code mapping, see [“X Key Codes Compared to Keysyms”](#) on page 329.

To configure keyboard mapping for a remote X server

- 1 Power off the virtual machine and close the Workstation window.
- 2 On the machine that hosts the virtual machine, add one of the following lines to the virtual machine configuration (.vmx) file or to ~/.vmware/config:
 - If you use an XFree86-based server that Workstation does not recognize as an XFree86 server, use the following property:

```
xkeymap.usekeycodeMap = "TRUE"
```

This property tells Workstation to always use key code mapping regardless of server type.

- If Workstation does recognize the remote server as an XFree86 server, use the following property:

```
xkeymap.usekeycodeMapIfXFree86 = "TRUE"
```

This property tells Workstation to use key code mapping if you are using an XFree86 server, even if it is remote.

- 3 Save and close the file.

Change How a Specific Key Is Mapped

If some keys on the keyboard do not work correctly in a virtual machine, you can set a property that makes a modification to the mapping.

Before you begin, perform the following tasks:

- Verify that the X server is an XFree86 server running on a PC. If the X server is remote, configure it to use key code mapping. See [“Configure Keyboard Mapping for a Remote X Server”](#) on page 327. For a description of key code mapping, see [“X Key Codes Compared to Keysyms”](#) on page 329.
- Determine the X key code and the corresponding v-scan code for the key. To find the X key code for a key, run `xev` or `xmodmap -pk`. Most v-scan codes are listed in [“V-Scan Code Table”](#) on page 331.

To change how a specific key is mapped

- 1 Power off the virtual machine and close the Workstation window.
- 2 On the machine that hosts the virtual machine, add the following line to the virtual machine configuration (.vmx) file or to `~/ .vmware/config`:

```
xkeymap.keycode.<code> = "<v-scan code>"
```

The `<code>` value must be a decimal number and `<v-scan code>` must be a C-syntax hexadecimal number (for example, `0x001`).

For example, to swap left Ctrl and Caps Lock, use the following lines:

```
xkeymap.keycode.64 = "0x01d # X Caps_Lock -> VM left ctrl"
xkeymap.keycode.37 = "0x03a # X Control_L -> VM caps lock"
```

- 3 Save and close the file.

X Key Codes Compared to Keysyms

Pressing a key on the PC keyboard generates a PC scan code based roughly on the position of the key. For example, the Z key on a German keyboard generates the same code as the Y key on an English keyboard because they are in the same position on the keyboard. Most keys have one-byte scan codes, but some keys have two-byte scan codes with prefix 0xe0.

Internally, Workstation uses a simplified version of the PC scan code that is a single nine-bit numeric value, called a v-scan code. A v-scan code is written as a three-digit hexadecimal number. The first digit is 0 or 1. For example, the Ctrl key on the left side of the keyboard has a one-byte scan code (0x1d). Its v-scan code is 0x01d. The Ctrl key scan code on the right side of the keyboard is two bytes (0xe0, 0x1d). Its v-scan code is 0x11d.

For an XFree86 server on a PC, there is a one-to-one mapping from X key codes to PC scan codes, or v-scan codes, which is what Workstation really uses. When Workstation is hosted on an XFree86 server and runs a local virtual machine, it uses the built-in mapping from X key codes to v-scan codes. This mapping is keyboard independent and should be correct for most languages. In other cases (not an XFree86 server or not a local server), Workstation must map keysyms to v-scan codes by using a set of keyboard-specific tables.

An X server uses a two-level encoding of keys, which includes the X key code and the keysym. An X key code is a one-byte value. The assignment of key codes to keys depends on the X server implementation and the physical keyboard. As a result, an X application normally cannot use key codes directly. Instead, the key codes are mapped into keysyms that have names like space, escape, x and 2. The mapping can be controlled by an X application by using the function `XChangeKeyboardMapping()` or by the program `xmodmap`. To explore keyboard mappings, you can use `xev`, which shows the key codes and keysyms for keys typed into its window.

A key code corresponds roughly to a physical key, whereas a keysym corresponds to the symbol on the key top. For example, with an XFree86 server running on a PC, the Z key on the German keyboard has the same key code as the Y key on an English keyboard. The German Z keysym, however, is the same as the English Z keysym, and different from the English Y keysym.

Configure How Keysyms Are Mapped

When key code mapping cannot be used or is disabled, Workstation maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation, you might need to set a property that tells Workstation which keysym table to use.

Before you begin, perform the following tasks:

- If you need to change the mapping of a few keys, determine the keysym name for each key that is not mapped correctly.

The easiest way to find the keysym name for a key is to run `xev` or `xmodmap -pk`. The X header file `/usr/include/X11/keysymdef.h` has a complete list of keysyms. The name of a keysym is the same as its C constant without the `XK_` prefix.

- If you need to use a different keysym table, determine which mapping table to use.

The tables are located in the `xkeymap` directory in the Workstation installation directory (usually `/usr/lib/VMware`). Which table you must use depends on the keyboard layout. The normal distribution includes tables for PC keyboards for the United States and a number of European countries and languages. And for most of these, there are both the 101-key (or 102-key) and the 104-key (or 105-key) variants.

- If none of the mapping tables is completely correct, find one that works best, copy it to a new location, and change the individual keysym mappings.

Workstation determines which table to use by examining the current X keymap. However, its decision-making process can sometimes fail. In addition, each mapping is fixed and might not be completely correct for any given keyboard and X key code-to-keysym mapping. For example, a user might have swapped Ctrl and Caps Lock using `xmodmap`. This means the keys are swapped in the virtual machine when using a remote server (keysym mapping) but are unswapped when using a local server (key code mapping). You can correct this situation by using configuration settings.

To configure how keysyms are mapped

- 1 Power off the virtual machine and close the Workstation window.
- 2 On the machine that hosts the virtual machine, add one or more of the following lines to the virtual machine configuration (`.vmx`) file or to `~/VMware/config`:

- To disable X key code mapping in order to map keysyms rather than key codes to v-scan codes, set the following property:

```
xkeymap.nokeycodeMap = "TRUE"
```

For more information, see [“X Key Codes Compared to Keysyms”](#) on page 329.

- If Workstation has a table in the `xkeymap` directory for your keyboard but cannot detect it, set the following property:

```
xkeymap.language = "<keyboard_type>"
```

The value `<keyboard_type>` must specify one of the tables in the `xkeymap` directory. However, the failure to detect the keyboard probably means the table is not completely correct for you. You might need to create a modified table and use the `xkeymap.fileName` property, described next.

- To use a different keysym mapping table that is not in the `xkeymap` directory, set the following property:

`xkeymap.fileName = "<file_path>"`

where `<file_path>` is the path to the table. The table must list a keysym for each key by using the following form:

`<sym> = "<v-scan code>"`

where `<sym>` is an X keysym name, and `<v-scan code>` is a C-syntax hexadecimal number (for example, `0x001`). Use a new line for each keysym.

Compiling a complete keysym mapping is difficult. VMware recommends editing an existing table and making small changes.

- To change the keysym mapping of a few keys, set the following property for each key, on separate lines:

`xkeymap.keysym.<sym> = "<v-scan code>"`

The value `<sym>` must be an X keysym name and `<v-scan code>` is a C-syntax hexadecimal number (for example, `0x001`).

Most v-scan codes are listed in [“V-Scan Code Table”](#) on page 331. The `xkeymap` tables themselves are also helpful.

3 Save and close the file.

V-Scan Code Table

[Table 18-1](#) shows the v-scan codes for the 104-key U.S. keyboard.

Table 18-1. V-Scan Codes for the 104-Key U.S. Keyboard

Symbol	Shifted Symbol	Location	V-Scan Code
Esc			0x001
1	!		0x002
2	@		0x003
3	#		0x004
4	\$		0x005
5	%		0x006

Table 18-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
6	^		0x007
7	&		0x008
8	*		0x009
9	(0x00a
0)		0x00b
-	_		0x00c
=	+		0x00d
Backspace			0x00e
Tab			0x00f
Q			0x010
W			0x011
E			0x012
R			0x013
T			0x014
Y			0x015
U			0x016
I			0x017
O			0x018
P			0x019
[{		0x01a
]	}		0x01b
Enter			0x01c
Ctrl		left	0x01d
A			0x01e
S			0x01f
D			0x020
F			0x021
G			0x022
H			0x023

Table 18-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
J			0x024
K			0x025
L			0x026
;			0x027
'			0x028
`			0x029
Shift		left	0x02a
\			0x02b
Z			0x02c
X			0x02d
C			0x02e
V			0x02f
B			0x030
N			0x031
M			0x032
,	<		0x033
.	>		0x034
/	?		0x035
Shift		right	0x036
*		numeric pad	0x037
Alt		left	0x038
Space bar			0x039
Caps Lock			0x03a
F1			0x03b
F2			0x03c
F3			0x03d
F4			0x03e
F5			0x03f
F6			0x040

Table 18-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
F7			0x041
F8			0x042
F9			0x043
F10			0x044
Num Lock		numeric pad	0x045
Scroll Lock			0x046
Home	7	numeric pad	0x047
Up arrow	8	numeric pad	0x048
PgUp	9	numeric pad	0x049
-		numeric pad	0x04a
Left arrow	4	numeric pad	0x04b
5		numeric pad	0x04c
Right arrow	6	numeric pad	0x04d
+		numeric pad	0x04e
End	1	numeric pad	0x04f
Down arrow	2	numeric pad	0x050
PgDn	3	numeric pad	0x051
Ins	0	numeric pad	0x052
Del		numeric pad	0x053
F11			0x057
F12			0x058
Break	Pause		0x100
Enter		numeric pad	0x11c
Ctrl		right	0x11d
/		numeric pad	0x135
SysRq	Print Scrn		0x137
Alt		right	0x138
Home		function pad	0x147
Up arrow		function pad	0x148

Table 18-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
Page Up		function pad	0x149
Left arrow		function pad	0x14b
Right arrow		function pad	0x14d
End		function pad	0x14f
Down arrow		function pad	0x150
Page Down		function pad	0x151
Insert		function pad	0x152
Delete		function pad	0x153
Windows		left	0x15b
Windows		right	0x15c
Menu			0x15d

The 84-key keyboard has a Sys Req key on the numeric pad. Its v-scan code is 0x054.

Keyboards outside the U.S. usually have an extra key (often <> or <> |) next to the left shift key. The v-scan code for this key is 0x056.

Using USB Devices in a Virtual Machine

Workstation provides a two-port USB controller, so that you can connect to both USB 1.1 and USB 2.0 devices:

- For USB 1.1, a UHCI controller with a virtual hub enables you to connect to more than two USB 1.1 devices.
- For USB 2.0, an EHCI controller enables you to connect to up to six USB 2.0 devices. For USB 2.0 support, your host must support USB 2.0, and you must enable USB 2.0 support in Workstation. USB 2.0 devices include high-speed or isochronous devices such as webcams, speakers, and microphones.

USB 2.0 support is available only for Workstation 6 and higher virtual machines.

On the host, when a USB 2.0 device connects to a port, the device connects to the EHCI controller and operates in USB 2.0 mode. A USB 1.1 device is automatically connected to a UHCI controller and operates in USB 1.1 mode. In Workstation 6 and higher virtual machines, this behavior is simulated if you enabled it. See [“Enable the USB 2.0 Controller for a Virtual Machine”](#) on page 336.

Although your host operating system must support USB, you do not need to install device-specific drivers for USB devices in the host operating system to use those devices only in the virtual machine. Windows NT and Linux kernels older than 2.2.17 do not support USB.

VMware has tested a variety of USB devices with this release. If the guest operating system has appropriate drivers, you can use PDAs, printers, storage (disk) devices, scanners, MP3 players, digital cameras, and memory card readers.

USB human interface devices, such as the keyboard and mouse, are not handled through the virtual machine's USB controller. Instead, they appear in the virtual machine as a standard PS/2 keyboard and mouse, even though they are plugged into USB ports on the host.

Enable the USB 2.0 Controller for a Virtual Machine

The virtual machine's USB ports are enabled by default, although support for high-speed USB 2.0 devices is not enabled by default. Modems and certain streaming data devices, such as speakers and webcams, do not work properly unless you enable USB 2.0 support.

Before you begin, perform one of the following tasks that apply to your setup:

- Verify that the virtual machine is a Workstation 6 or higher virtual machine.
- On Windows XP guests, verify that the latest service pack is installed if you want to use USB 2.0.

If you use Windows XP with no service packs, the driver for the EHCI controller cannot be loaded.

- On a Windows 2000 host with USB 2.0 support, use the Microsoft USB 2.0 driver for the USB controller.

Third-party USB 2.0 drivers, such as those provided by some motherboard manufacturers, are not supported. For notes on replacing the third-party drivers, see [“Replace USB 2.0 Drivers on a Windows 2000 Host”](#) on page 339.

If you do not plan to use USB devices in a virtual machine, you can disable (or enable) USB 2.0 support by using the virtual machine settings editor.

To enable the USB 2.0 Controller for a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.

- 4 On the **Hardware** tab, select **USB Controller**.
- 5 Select the **Enable high-speed support for USB 2.0 devices** check box and click **OK**.

Add a USB Controller to a Virtual Machine

By default a USB controller is included when you create a virtual machine. If you remove the USB controller, you can add it back.

This controller is required to use a smart card in a virtual machine regardless of whether the smart card reader is a USB device.

To add a USB controller to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
- 5 On the Hardware Type page, select **USB Controller** and click **Next**.
- 6 On the USB page, click **Finish**.
- 7 In the virtual machine settings editor, click **OK**.

You can now start the virtual machine and automatically or manually connect USB devices and smart card readers.

Connecting USB Devices

When a virtual machine is running, its window is the active window. If you plug a USB device into the host, by default, the device connects to the virtual machine instead of the host.

If you manually connect a USB device to a virtual machine (by choosing **VM > Removable Devices**), Workstation retains the virtual machine's connection to the affected port on the host. You can suspend or power off the virtual machine, or unplug the device. When you plug the device back in or resume the virtual machine, Workstation reconnects the device. Workstation retains the connection by writing an autoconnect entry to the virtual machine's configuration (.vmx) file.

If Workstation is unable to reconnect to the device (for example, because you disconnect the device), the device is removed and a message is displayed, indicating that

Workstation is unable to connect to the device. You can connect manually to the device if it is still available.

Enable or Disable Automatic Connection of USB Devices

You can disable the autoconnect feature if you do not want USB devices to automatically connect to the virtual machine when you power it on.

To enable or disable automatic connection of USB devices

- 1 Select the virtual machine.
The virtual machine can be powered on or off.
- 2 Choose **VM > Settings**.
- 3 On the **Hardware** tab, select **USB Controller**.
- 4 Use the **Automatically connect new USB devices to this virtual machine when it has focus** check box to enable or disable the setting and click **OK**.

Connect a USB Device Manually

If a device that is connected to the host does not automatically connect to a virtual machine at power on, you can connect the device manually.

Also, when you are using a virtual machine, if you plug a device in to the host, the autoconnect feature usually connects the device to the virtual machine. If this action does not occur, you can connect the device manually.

To connect a USB device manually

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered on.
- 3 Choose **VM > Removable Devices > <device_name>**.

Here **<device_name>** specifies the USB device that is plugged in to the host. A check mark appears next to the device's name, indicating that it is connected.

If the physical USB devices are connected to the host through a hub, the virtual machine sees only the USB devices, not the hub.

USB Driver Installation on a Windows Host

When a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver.

On Windows XP and Windows Server 2003 hosts, the Microsoft Windows Found New Hardware wizard prompts you to run it. Select the default action, **Install the software automatically**. After the software is installed, the guest operating system detects the USB device and searches for a suitable driver.

When you synchronize a PDA, such as a Palm handheld or Handspring Visor, to a virtual machine for the first time, the total time required to load the VMware USB device driver in the host and the PDA driver in the guest might exceed the device's connection timeout value. This causes the device to disconnect itself from the computer before the guest can synchronize with it. If this occurs, let the guest finish installing the PDA driver, dismiss any connection error warnings, and try synchronizing the PDA again. The second attempt should succeed.

Replace USB 2.0 Drivers on a Windows 2000 Host

To use Workstation on a Windows 2000 host that has USB 2.0 ports, you must use the Microsoft USB 2.0 drivers for the USB controller in the host operating system. If your host operating system is using a third-party driver—a driver supplied by your motherboard vendor, for example—you must replace it.

To replace USB 2.0 drivers on a Windows 2000 host

- 1 To determine the provider of the USB driver, open the Device Manager, as follows:
 - a Right-click **My Computer** and choose **Properties**.
 - b Click the **Hardware** tab and click **Device Manager**.
- 2 Expand the listing for Universal Serial Bus controllers.
- 3 Right-click the listing for the controller and choose **Properties**.
- 4 Click the **Driver** tab.

If the driver provider shown on the tab is Microsoft, you have the correct driver and do not need to replace it.

- 5 If the driver provider is not Microsoft, download and install the latest USB driver for your host operating system from the Microsoft Web site.

Details are available in Microsoft knowledge base article 319973.

Access and Use a USB Device on a Linux Host

On Linux hosts, Workstation uses the USB device file system to connect to USB devices. In most Linux systems that support USB, the USB device file system is located in `/proc/bus/usb`.

If the host uses a different path to the USB device file system, you must mount the USB file system to the expected location.

To access and use a USB device on a Linux host

- 1 Run the following command as root:

```
mount -t usbfs none /proc/bus/usb
```

- 2 If the virtual machine does not have a USB controller, add it by using the Add Hardware wizard in Workstation.

Do not attempt to add a USB drive's device node directory (for example, `/dev/sda`) to the virtual machine as a hard disk. See [“Add a USB Controller to a Virtual Machine”](#) on page 337.

How Device Control Is Shared Between Host and Guest

Only the host or the guest can have control of a USB device at any one time. Device control operates differently, depending on whether the host is a Linux or a Windows computer.

Device Control on a Windows Host

When you connect a device to a virtual machine, it is “unplugged” from the host or from the virtual machine that previously had control of the device. When you disconnect a device from a virtual machine, it is “plugged in” to the host.

Under some circumstances, if a USB storage device is in use on the host (for example, one or more files stored on the device are open on the host), an error appears in the virtual machine when you try to connect to the device. You must let the host complete its operation or close any application connected to the device on the host, and then connect to the device in the virtual machine again.

On Windows 2000, Windows XP, and Windows Server 2003 hosts, when you connect a USB network or storage device to a virtual machine, you might see a message on your host that says the device can be removed safely. This is normal behavior, and you can dismiss the dialog box. However, do *not* remove the device from your physical computer.

If the network or storage device does not disconnect from the host, use the appropriate system tray icon to disconnect it. On Windows 2000, the icon is called **Eject Hardware**. On Windows XP and Windows Server 2003, it is called **Safely Remove Hardware**.

Troubleshoot Device Control Issues on a Linux Host

On Linux hosts, guest operating systems can use devices that are not already in use by the host—that is, devices that are not claimed by a host operating system driver.

If the device is in use by the host and you try to connect it to the guest by using the **VM > Removable Devices** menu, a dialog box appears, asking whether you want to disconnect the driver on the host. Occasionally, disconnecting the device fails.

A related issue sometimes affects devices that rely on automatic connection (as PDAs often do). Occasionally, even if you successfully used autoconnection to connect the device to the virtual machine, you might experience problems with the connection to the device.

To troubleshoot device control issues on a Linux host

- 1 If you have problems with automatic connections, use the **VM > Removable Devices** menu to disconnect the device and reconnect it.
- 2 If the problem persists, unplug the device physically and plug it in again.
- 3 If you see a dialog box warning that the device is in use, disable it in the **hotplug** configuration files in the `/etc/hotplug` directory.

See your Linux distribution's documentation for details on editing these configuration files.

- 4 If a disconnection fails, do one of the following, as appropriate:
 - If the driver was automatically loaded by **hotplug**, disable it in the **hotplug** configuration files in the `/etc/hotplug` directory.
See your Linux distribution's documentation for details on editing these configuration files.
 - Unload the device driver manually as root (`su -`) by using the `rmmod` command.

Disconnecting USB Devices from a Virtual Machine

Before unplugging a USB device or using the **VM > Removable Devices** menu to disconnect it from a virtual machine, be sure it is in a safe state.

Follow the procedures the device manufacturer specifies for unplugging the device from a physical computer. This is true whether you are physically unplugging it, moving it from host to virtual machine, moving it between virtual machines, or moving it from virtual machine to host.

This is important with data storage devices (a Zip drive, for example). If you move a data storage device too soon after saving a file and the operating system has not actually written the data to the disk, you can lose data.

Use Smart Cards with Virtual Machines

A smart card is a plastic card about the size of a credit card but embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. Users plug a smart card reader into their computer and then insert their smart card in the reader. They are then prompted for credentials in order to log on to the network.

Smart card readers are considered a type of USB device by the virtual machine. You can therefore use the **VM > Removable Devices** menu to access them. Virtual machines can connect to smart card readers that interface to serial ports, parallel ports, USB ports, PCMCIA slots, and PCI slots.

To use a host's smart card reader in a virtual machine, make sure the following prerequisites are satisfied:

- On Windows hosts, start the service called `SCardSvr.exe` if it is not already running.
- On Linux hosts, make sure the `libpcsclite` library is installed. Most recent Linux distributions include this library.
- Make sure the virtual machine has a USB controller.

A USB controller is required regardless of whether the smart card reader itself is a USB device. By default USB controllers are included when you create a virtual machine. If you removed the USB controller, you must add it back. See [“Add a USB Controller to a Virtual Machine”](#) on page 337.

To use smart cards with virtual machines

- 1 Connect the smart card reader to the host machine.
- 2 Start the virtual machine.
- 3 To connect the smart card reader to a virtual machine, use the **VM > Removable Devices** menu.

The smart card reader is now shared by the host and the virtual machine. The smart card reader can also be shared by multiple virtual machines.

Support for Generic SCSI Devices

Generic SCSI gives the guest operating system direct access to SCSI devices connected to the host, such as scanners, tape drives, and other data storage devices. Using the SCSI generic driver, Workstation allows a virtual machine to run any SCSI device that is supported by the guest operating system.

In theory, generic SCSI is completely device independent, but VMware has discovered it is sensitive to the guest operating system, device class, and specific SCSI hardware. Try any SCSI hardware and report problems to VMware technical support.

On Windows hosts, to access host SCSI devices from within a virtual machine, you must run Workstation as a user with administrator access.

On Linux hosts, you must have read and write permissions on a given generic SCSI device to use the device within a virtual machine, even if the device is a read-only device such as a CD-ROM drive. These devices typically default to root-only permissions. Your administrator can create a group with access to read and write to these devices and add the appropriate users to that group.

Installing Required Adapters or Drivers for Some Windows Guests

On older Windows guest operating systems, you might need to install special host bus adapters. It also contains information about a special SCSI driver for 32-bit Windows XP guests.

Installing a SCSI Adapter on Windows 9.x and Me Guests

If you use generic SCSI devices in a Windows 95, Windows 98, or Windows Me guest operating system and are experiencing problems with the devices, download the latest Mylex (BusLogic) BT/KT-958 compatible host bus adapter from LSI Web site. Follow the instructions on the Web site to install the driver.

This driver overrides what Windows chooses as the best driver, but it corrects known problems.

Installing a SCSI Driver for 32-Bit Windows XP Guests

To use SCSI devices in a 32-bit Windows XP virtual machine, you need a special SCSI driver available from the Download page of the VMware Web site. Follow the instructions on the Web site to install the driver.

Install the BusLogic Driver in a Windows NT 4.0 Guests

Generic SCSI devices use the virtual Mylex (BusLogic) BT/KT-958 compatible host bus adapter provided by the virtual machine. On Windows NT 4.0, you might need to install the driver manually, if it is not already installed for a virtual SCSI disk. Do so before you add a generic SCSI device.

Before you begin, have your Windows NT installation CD available.

To install the BusLogic driver in a Windows NT 4.0 guest

- 1 To open the SCSI Adapters control panel, choose **Start > Settings > Control Panel > SCSI Adapters**.
- 2 On the **Drivers** tab, click **Add**.
- 3 In the list of vendors on the left, select **BusLogic**.
- 4 In the list of drivers on the right, select **BusLogic MultiMaster PCI SCSI Host Adapters** and click **OK**.
- 5 Insert the Windows NT CD when you are prompted and click **OK**.
- 6 Reboot when you are prompted.

Avoiding Concurrent Access on Linux Hosts

The SCSI generic driver sets up a mapping for each SCSI device in `/dev`. Each entry starts with `sg` (for the SCSI generic driver) followed by a letter. For example, `/dev/sg0` is the first generic SCSI device. Each entry corresponds to a SCSI device in the order specified in `/proc/scsi/scsi`, from the lowest device ID on the lowest adapter to the highest device ID on the lowest adapter, and so on to the highest device ID on the highest adapter.

Some Linux devices such as tape drives, disk drives, and CD-ROM drives, already have a designated `/dev` entry (`st`, `sd`, and `sr`, respectively). When the SCSI generic driver is installed, Linux identifies these devices with corresponding `sg` entries in `/dev` in addition to their traditional entries. Workstation ensures that multiple programs are not using the same `/dev/sg` entry at the same time but cannot always ensure that multiple programs are not using the `/dev/sg` entry and the traditional `/dev` entry at the same time. When you specify which SCSI device to use in a virtual machine, do not specify `/dev/st0` or `/dev/sr0`.



CAUTION Do not attempt to use the same generic SCSI device in both host and guest. This can cause unexpected behavior and might cause loss or corruption of data.

Add a Generic SCSI Device to a Virtual Machine

To map virtual SCSI devices on a virtual machine to physical generic SCSI devices on the host, you must add a generic SCSI device to the virtual machine.

Before you begin, make sure you have the following required permissions:

- On Windows hosts, to access host SCSI devices as generic SCSI devices, you must run Workstation as a user with administrator access.
- On Linux hosts, generic SCSI requires version 2.1.36 or higher of the SCSI Generic (sg.o) driver, which comes with kernel 2.2.14 and higher. Also, you must be logged on as a user who has permissions to use the device (that is, read and write permissions).

To add a generic SCSI device to a virtual machine

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
- 5 On the Hardware Type page, select **Generic SCSI Device** and click **Next**.
- 6 On the Choose SCSI Device page, from the drop-down list of SCSI devices, select the physical device to map.

If you do not see the device you want in the list, you might need to add it manually, as described in [“Troubleshoot Issues with Detecting Generic SCSI Devices”](#) on page 346.

On Linux hosts, if you type in the path to the SCSI device, do not enter `/dev/st0` or `/dev/sr0`.

- 7 Use the **Connect at power on** check box to configure automatic connection behavior and click **Finish**.
- 8 On the **Hardware** tab, in the **Virtual device node** section, select the SCSI device identifier to use for the drive and click **OK**.

For example, if you select SCSI 0:2, the guest operating system sees the drive as ID 2 on controller 0.

Troubleshoot Issues with Detecting Generic SCSI Devices

When you use the virtual machine settings editor to add a generic SCSI device to a virtual machine, occasionally the device does not appear in the list of available SCSI devices. This topic describes how to resolve this issue.

Before you begin troubleshooting this problem, you might need to know the following:

- The SCSI bus number the device uses on the host system. The SCSI bus is assigned a number by the host operating system after all IDE buses have been assigned numbers. For example, if you have two IDE buses, they are numbered 0 and 1. The first SCSI bus is assigned bus number 2.

If you cannot determine the SCSI bus number, try using a third-party tool such as `winobj` to determine this information. You can download `winobj` for free from the Windows Sysinternals Web site.

- The target ID the device uses in the virtual machine and on the host. This ID is usually set by some jumpers or switches on the device. Refer to the owner's manual for the device for information on how to determine the target ID.

The root causes or reasons Workstation cannot detect a device include the following:

- A driver for that device is not installed on the host.
- A driver on the host prevents the device from being detected.
- The virtual machine uses a device for which there are no drivers available to the host operating system. In this case, you need to add the device manually to the virtual machine's configuration (`.vmx`) file. Adding a device in this manner is recommended for advanced users only.

To troubleshoot issues with detecting generic SCSI devices

- 1 Find out whether the device driver for this device is installed on the host.
- 2 If the device driver is not installed and you want to install it, do so and see if the device appears correctly in the virtual machine settings editor.

You might not want to install the driver on the host if you want to avoid a device-in-use conflict between the host and guest.

If a driver is installed but does not appear correctly, or if you cannot install the driver on the host, or if you do not want to install the driver on the host, add the device manually to the virtual machine, as described in the rest of this procedure.

- 3 If an original SCSI device driver is already installed on the host, disable it.

Some Windows operating systems do not process the send command from the adapter if the device driver is owning the device.

- 4 Power off the virtual machine, and open the virtual machine's configuration (.vmx) file in a text editor.

- 5 Add or change the following line in the .vmx file:

```
scsiZ:Y.fileName = "<deviceName>"
```

where *X* is the SCSI bus number the device uses on the host system, and *Y* is the target ID the device uses both in the virtual machine and on the host. For

"<deviceName>" use:

```
"scsiX:Y"
```

Here is an example of how to set the option. Say the problematic device is a CD-ROM drive, and the existing entry in the configuration file is:

```
scsi0:4.fileName = "CdRom0"
```

If the device on the host is located on bus 2 with target ID 4, change this line to:

```
scsi0:4.fileName = "scsi2:4"
```

If your problem was that the virtual machine has a SCSI adapter and generic SCSI device, but Workstation did not recognize the device when the virtual machine was powered on, you can stop at this point.

- 6 If the virtual machine does not contain any SCSI devices, or if you want to add a generic SCSI device to a new virtual SCSI adapter, or if you want to use an existing SCSI device as a generic SCSI device, also add the following line in the .vmx file:

```
scsiZ:Y.deviceType = "scsi-passthru"
```

If your problem was that you want to use an existing SCSI device as a generic SCSI device, you can stop at this point.

- 7 If the virtual machine does not contain any SCSI devices, or if you want to add a generic SCSI device to a new virtual SCSI adapter, also add the following lines in the .vmx file:

```
scsiZ:Y.present = "true"
```

```
scsiZ.present = "true"
```

where *Z* is the SCSI bus number the device uses in the virtual machine.

If the virtual machine settings editor still does not include this device in the list of available SCSI devices for this virtual machine, contact VMware technical support.

Use Two-Way Virtual Symmetric Multiprocessing

With virtual SMP, you can assign two virtual processors to a virtual machine on any host machine that has at least two logical processors.

The following are all considered to have two or more logical processors:

- A multiprocessor host with two or more physical CPUs
- A single-processor host with a multicore CPU
- A single-processor host with hyperthreading enabled

NOTE On hyperthreaded uniprocessor hosts, performance of virtual machines with virtual SMP might be subpar.

Guests with more than two virtual processors are not supported in Workstation. However, you can power on and run multiple dual-processor virtual machines concurrently.

The number of virtual processors for a given virtual machine is displayed in the summary view of the virtual machine.

To use two-way virtual symmetric multiprocessing

Depending on whether you are creating a new virtual machine or configuring an existing one, do one of the following:

- For a new virtual machine, choose the custom configuration in the New Virtual Machine wizard and when you come to the Processor Configuration page, specify the number.
- For an existing virtual machine, choose **VM > Settings** and on the **Hardware** tab, select **Processors** and specify the number.

Use a Virtual Machine That Originally Had More Than Two Virtual Processors

You can use Workstation 6.5 or higher, running on a multiprocessor host machine, to open a virtual machine created in VMware ESX Server that has one or more virtual processors. You cannot use Workstation, however, to power on a virtual machine that has more than two virtual processors assigned, even if more processors were assigned when the virtual machine was created in ESX Server.

You can see the number of processors in the virtual machine's summary view or by using the virtual machine settings editor. To use a virtual machine that has more than two virtual processors assigned, you must change the number of processors before powering it on.

To use a virtual machine that originally had more than two virtual processors

- 1 Select the virtual machine.
- 2 Make sure the virtual machine is powered off.
- 3 Choose **VM > Settings**.
- 4 On the **Hardware** tab, select **Processors**, and note that **Number of Processors** is set to **Other (x)**, where **x** is the number of processors originally assigned in ESX Server.

Workstation preserves this original configuration setting for the number of processors, even though two is the maximum number of processors supported. You must change this setting to one or two processors before you can power on the virtual machine in Workstation.

After you commit a change to this setting, the original setting for number of processors is discarded and no longer appears as an option in the virtual machine settings editor.

- 5 Change the **Number of processors** setting to **One** or **Two** and click **OK**.

BETA

Special-Purpose Configuration Options for Windows Hosts

19

You can use configuration options for tasks like restricting the operations a user can perform with a virtual machine or simplifying the user interface for inexperienced users. In a classroom, for example, you can ensure that virtual machine configurations remain consistent from one class session to the next.

This chapter includes the following topics:

- [“Locking Out Interface Features for Windows Hosts Only”](#) on page 351
- [“Restricting the User Interface”](#) on page 352
- [“Using Full-Screen Switch Mode for Windows Hosts Only”](#) on page 355
- [“Guest ACPI S1 Sleep”](#) on page 365

Locking Out Interface Features for Windows Hosts Only

Administrative lockout is a global setting that affects all virtual machines for all users on a host computer. It allows you to configure settings so that only a user who knows the password can perform the following tasks:

- Create new virtual machines.
- Edit virtual machine configurations.
- Edit network settings.

If no user has set administrative lockout preferences, any user can set them and set a password for access to the administrative lockout features. If administrative lockout preferences are already set by any user, you must know the password to change the settings.

Set Administrative Lockout Preferences

To set administrative lockout preferences

- 1 Choose **Edit > Preferences**.
- 2 Click the **Lockout** tab and enter the password if prompted.
You are prompted for a password if a user has already set administrative lockout preferences.
- 3 Select the **Enable** check box and select the actions you want to restrict.
If this is the first time administrative lockout options are being set, specify a password in the fields provided.
- 4 Click **OK**.
The settings are saved.

Removing a Forgotten Password

If you cannot remember the password and need to remove it, you must uninstall Workstation. Be sure to click **Yes** when asked if you want to remove the administrative lockout settings. After you reinstall Workstation, you can enable the administrative lockout features and set a new password.

Restricting the User Interface

To enable the restricted user interface a user must have sufficient privileges to edit the virtual machine's configuration file and to set file permissions. The restricted user interface affects only the specific virtual machines for which the setting is created.

The following changes occur when you enable the restricted user interface:

- The toolbar is always hidden.
- All functions on the **VM > Power** menu are disabled.
- All functions on the **VM > Snapshot** menu and snapshot functions on the toolbar are disabled.
- No access is provided to the virtual machine settings editor (**VM > Settings**) from the VMware Workstation window.
- The user cannot change virtual networking settings (**Edit > Virtual Network Settings**).

- The user starts the virtual machine by double-clicking the configuration file (.vmx file) or a desktop shortcut to that file and the virtual machine powers on. At the end of the working session, the user shuts down by closing the virtual machine (**File > Exit**).

It is also possible to launch Workstation and open a restricted-interface virtual machine from the virtual machine list or the **File** menu.

Enable the Restricted User Interface

Although the restricted user interface provides no access to menu and toolbar controls for a snapshot, you can give users limited snapshot control. If you set up a snapshot for the restricted virtual machine and set the power-off option to **Ask Me**, the standard dialog box appears when a virtual machine shuts down and the user can choose **Just Power Off**, **Take Snapshot**, or **Revert to Snapshot**.

To enable the restricted user interface

- 1 Power off the virtual machine and close the VMware Workstation window.
- 2 Open the virtual machine's configuration file (.vmx file) in a text editor.
- 3 Add the following line anywhere in the file:
`gui.restricted = "TRUE"`
- 4 (Optional) Set file permissions on the configuration file to give normal users of the system only read access to the file.

This prevents normal users from manually modifying the configuration.
- 5 Create a shortcut to the configuration file on the desktop and give it an appropriate name.

Return to a Snapshot with Restricted User Interface

You can combine a restricted user interface with a snapshot to ensure that users' virtual machines always start in the same state. Typically, users running a virtual machine with a restricted user interface can only power it on and off, and the virtual machine boots when powered on. When the virtual machine has a snapshot set and is configured to return to that snapshot when powered off, the user can only start and power off the virtual machine. The virtual machine always starts from the snapshot.

To set up a virtual machine with a restricted user interface for Windows only

- 1 Power on the virtual machine and be sure it is in the appropriate state.
- 2 Create a snapshot.

See [“Take a Snapshot”](#) on page 195.

- 3 Configure the virtual machine to return to the snapshot any time it is powered off: Choose **VM > Settings > Options > Snapshot/Replay** and select **After Powering Off** and **Revert to Snapshot**.
- 4 With the virtual machine powered off, restrict the user interface, as follows:
 - a Close the VMware Workstation window.
 - b Open the virtual machine's configuration file (.vmx file) in a text editor.
 - c Add the following line anywhere in the file.


```
gui.restricted = "TRUE"
```
- 5 (Optional) Set file permissions on the configuration file to give normal users of the system read-only access to the file.

This prevents normal users from manually modifying the configuration.
- 6 Create a shortcut to the configuration file on the desktop and name it.
- 7 Run this virtual machine by double-clicking the shortcut to the configuration file.

The virtual machine starts at the snapshot, with the user interface restricted. Users do not have a toolbar or access to the **VM > Power** menu or the virtual machine settings editor.
- 8 Choose **File > Close**.

The virtual machine powers off, and the next time a user powers it on, it returns to the snapshot.

Disable Restricted User Interface

To disable the restriction on the interface

- 1 Power off the virtual machine and close the VMware Workstation window.
- 2 Open the configuration file (.vmx) file and do one of the following:
 - Set `gui.restricted = "FALSE"`.
 - Remove or comment out the `gui.restricted = "TRUE"` line.
- 3 Save the changes to the configuration file and close it.
- 4 Start the virtual machine by double-clicking the shortcut.

The virtual machine starts at the snapshot, and the interface is not restricted.

Using Full-Screen Switch Mode for Windows Hosts Only

Full-screen switch mode is a runtime option for the VMware Workstation program on Windows hosts. When Workstation is running in full-screen switch mode, the user has no access to the Workstation user interface. The user cannot create, reconfigure, or launch virtual machines. A system administrator performs these functions.

When Workstation is running in full-screen switch mode, one or more virtual machines can be running, and you can use hot keys to switch from one to another. You can also provide hot-key access to the host operating system.

Full screen switch mode is enabled for Windows hosts only. Linux hosts do not have full screen switch mode.

Create a Virtual Machine for Use in Full-Screen Switch Mode

To create virtual machines, run Workstation in standard mode. The instructions in this section assume that you are creating the virtual machines on a separate administrative computer. You can also create the virtual machines directly on the user's computer.

If you plan to run the virtual machine on a laptop computer, be sure to set the virtual machine to report the battery status, as described in [“Report Battery Information in the Guest Operating System”](#) on page 158.

Create a virtual machine by following the instructions in [“Create a Virtual Machine by Using the Custom Setup”](#) on page 94.

As you complete the New Virtual Machine wizard, make the following choices:

- On the Name the Virtual Machine page, make a note of the folder in which you create the virtual machine. You must copy all the files in this folder to the user's computer after you finish creating and configuring the virtual machine.
- On the Specify Disk Capacity page, specify the size for the virtual disk and select **Allocate all disk space now**. VMware strongly recommends this selection. If you do not make this selection and the host computer's hard disk runs out of space for a growing virtual disk file, the user sees no warning message and does not know what is causing the problem in the virtual machine.

To create a virtual machine for use in full-screen switch mode

- 1 To open the virtual machine settings editor, select the virtual machine and choose **VM > Settings**.
- 2 Use the virtual machine settings editor to make all needed configuration settings before you configure the user's computer to launch Workstation when the computer starts.

You cannot change virtual machine settings by using the virtual machine settings editor when Workstation is running in full-screen switch mode. VMware recommends that you finish configuring the virtual machine and install the guest operating system and applications before you move the virtual machine to a user's computer.

Moving a Virtual Machine to a User's Computer

The easiest way to move the virtual machine to a user's computer is to use a network connection to copy all the files in the virtual machine directory to a directory on the user's computer. You can also move the directory by using a DVD or other removable media large enough to store the files.

Place each virtual machine in its own separate directory.

Configuring Full-Screen Switch Mode

You can configure full-screen switch mode to specify hot keys for cycling through the currently powered-on virtual machines, to switch to a specific virtual machine or the host, and more.

Global Configuration Settings

To use full-screen switch mode, you must, set the `msg.autoAnswer` property in the Workstation global configuration file. This setting causes Workstation to suppress any Workstation dialog boxes that otherwise appear. The default answer is selected in these dialog boxes.

The global configuration file created when you change any of the default settings in the Workstation preferences editor (**Edit > Preferences**). The file location depends on the host operating system:

- On most Windows hosts:

`C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation\config.ini`

- On Windows Vista hosts:

`C:\Users\All Users\Application Data\VMware\VMware Workstation\config.ini`

Full-screen switch mode is enabled for Windows hosts only. On Linux, the configuration file is located in `/etc/vmware/config`

Specify Global Configuration Settings for Full-Screen Switch Mode

To specify global configuration settings for full-screen switch mode

- 1 If the `config.ini` file does not yet exist on your host computer, choose **Edit > Preferences** from the Workstation menu bar and change at least one of the settings in the preference editor.

- 2 Open the `config.ini` file with a text editor and add the following line:

```
msg.autoAnswer = "TRUE"
```

- 3 (Optional) Specify other full-screen switch mode settings you want to use.

To specify hot keys for switching to other virtual machines or the host computer, first, see the following sections, in the order listed:

- [“Virtual Key Codes”](#) on page 357
- [“Hot Key for Cycling Through Virtual Machines and the Host Computer”](#) on page 359
- [“Host Operating System Hot Key”](#) on page 360
- [“Other Entries in the Global Configuration File”](#) on page 360.

- 4 Save and close the file.
- 5 Set permissions on this file so that other users cannot change it.
- 6 Open the `preferences.ini` file with a text editor and add the following lines:

```
pref.fullScreen.v5 = "TRUE"
pref.autoFitFullScreen = "fitGuestToHost"
```

On most Windows hosts, this file is located in:

```
%USERPROFILE%\Application Data\VMware\preferences.ini
```

On Windows Vista hosts, this file is located in:

```
%USERPROFILE%\AppData\Roaming\VMware\preferences.ini
```

To specify a hot key for switching to a specific virtual machine, see [“Virtual Machine Hot Key”](#) on page 360.

Virtual Key Codes

The hot-key entries described in this section require you to enter a virtual key code as part of the value for an option. Virtual key codes use hexadecimal format, which is a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type **0x5A**.

Microsoft provides a reference list of virtual key codes. To access this reference list enter the keyword virtual key codes on the MSDN Web site.

The hot-key entries also include modifier keys. The modifier keys are Ctrl, Alt, Shift, and Windows keys. The Windows key is the key between the Ctrl and Alt keys. You can also use a combination of those keys. [Table 19-1](#) lists the key codes for the modifier keys.

Table 19-1. Modifier Keys for Hot-Key Entries

Modifier Key	Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Win (Windows)	0x8
Ctrl+Alt	0x3
Alt+Shift	0x5
Ctrl+Shift	0x6
Ctrl+Alt+Shift	0x7
Win+Alt	0x9
Win+Ctrl	0xa
Win+Ctrl+Alt	0xb
Win+Shift	0xc
Win+Shift+Alt	0xd
Win+Shift+Ctrl	0xe
Win+Shift+Ctrl+Alt	0xf

Keep the following limitations in mind when defining cycle keys and switch keys:

- Do not use the Pause key with the Ctrl key. You can use the Pause key with other modifier keys.
- If you use the F12 key, you must use one or more modifier keys. You cannot use the F12 key alone.
- You cannot use combinations that include only the Shift, Ctrl, and Alt keys. These keys can be used only as modifiers in combination with some other key.

When listing a key plus a modifier, type the virtual key code for the key followed by a comma and type the value for the modifier key or keys. For example, the value entry for Ctrl+Shift+F1 is 0x70,0x6.

Hot Key for Cycling Through Virtual Machines and the Host Computer

You can specify a hot key or hot-key combination for cycling through the available virtual machines on a host computer. Hot keys behave in the following manner:

- Each time you press the specified hot key, the next virtual machine appears in order. You can also include the host operating system in the cycle.
- If any particular virtual machine is not running, it is skipped.
- If only one virtual machine is running and the host operating system is not included in the cycle, pressing the hot key has no effect.

The hot key for cycling through virtual machines is defined in the global configuration file (`config.ini`). Two options control cycling:

■ `FullScreenSwitch.cycleKey`

The value of this option defines the hot key. It is specified as `<key>, <modifier>`. It has no default. For example, to use the Pause key with no modifier to cycle through virtual machines, add the following line to the `config.ini` file, or modify its value if the option is already listed:

```
FullScreenSwitch.cycleKey = "0x13,0x0"
```

■ `FullScreenSwitch.cycleHost`

Set this option to `TRUE` to include the host operating system in the cycle. The default is `FALSE`. For example, to include the host operating system in the cycle, add the following line to the `config.ini` file, or modify its value if the option is already listed:

```
FullScreenSwitch.cycleHost = "TRUE"
```

Hot Keys for Switching Directly to Virtual Machines and the Host Computer

You can specify a hot key or hot-key combination for switching directly to any available virtual machine on a host computer. Each time you press the specified hot key, the screen display switches to that of the specified virtual machine. You can also specify a hot key for switching directly to the host operating system.

Virtual Machine Hot Key

You define the hot key used to switch to a virtual machine by adding a local configuration setting. Local configuration settings are made in the configuration file for a particular virtual machine. The local configuration file is in the virtual machine's directory. The filename has a `.vmx` extension.

Follow this format for an entry in either configuration file is:

```
<option> = "<value>"
```

Entries in the configuration files can appear in any order. The value of this option defines the hot key. It is specified as `<key>`, `<modifier>`. It has no default.

For example, to use Ctrl+Shift+F1 to switch to a particular virtual machine, add the following line to that virtual machine's `.vmx` file or modify its value if the option is already listed:

```
FullScreenSwitch.directKey = "0x70,0x6"
```

If any particular virtual machine is not running, pressing the hot key for that virtual machine has no effect.

Host Operating System Hot Key

You define the hot key used to switch to the host operating system by adding a line to the global configuration file (`config.ini`). The value of this option defines the hot key. It is specified as `<key>`, `<modifier>`. It has no default.

For example, to use Ctrl+Shift+F9 to switch to the host operating system, add the following line to the `config.ini` file, or modify its value if the option is already listed:

```
FullScreenSwitch.hostDirectKey = "0x78,0x6"
```

Other Entries in the Global Configuration File

The global configuration file (`config.ini`) entries in [Table 19-2](#) are optional. They enable you to control certain functions of the virtual machine that are important in

work environments where virtual machines need to be isolated from each other and from the host computer:

Table 19-2. Optional Global Configuration File Entries

Option	Description	Default Setting
Isolation.tools.copy.enable Isolation.tools.paste.enable	This option determines whether data in one virtual machine or the host operating system can be copied in a way that allows it to be transferred to another virtual machine or to the host operating system.	TRUE
Isolation.tools.paste.enable Isolation.tools.copy.enable	This option determines whether data copied in one virtual machine or the host operating system can be pasted into another virtual machine or the host operating system.	TRUE
Isolation.tools.HGFS.disable	The value of this option determines whether virtual machines can be configured with shared folders, for sharing files among virtual machines and with the host computer.	FALSE
mks.CtlAltDel.ignore	Set this property to TRUE so that dialog boxes usually generated by Microsoft Windows Secure Attention Sequence (SAS) are not displayed but are passed on to the guest if the guest has keyboard focus.	
mks.fullscreen.allScreenSaver	Set this property to TRUE to allow the host operating system to run its screen saver when it determines that the machine is idle.	

Starting and Stopping Virtual Machines on a User's Computer

Use the `vmware-fullscreen` command to run VMware Workstation in full-screen switch mode and to start and stop virtual machines on a user's computer. The command can pass certain information to the virtual machine when it starts.

As administrator, you must decide how to issue the command. For example, you can use a custom application or script running on the host operating system to issue one or more `vmware-fullscreen` commands. Or you can include the command to start a virtual machine in a shortcut in the host operating system's startup group, so the virtual machine starts when the user logs in to the host computer.

Issue the `vmware-fullscreen` command once for each virtual machine you want to start or stop.

Start a Virtual Machine

- 1 Enter the `vmware-fullscreen` command to power on a virtual machine:

```
vmware-fullscreen -poweron "<config-file>"
```

- 2 Provide the full path to the virtual machine's configuration (.vmx) file.

The user sees no immediate indication when the virtual machine starts, but the user can switch to the virtual machine with its direct-switch key or with the cycle key.

- 3 To power on the virtual machine and pass additional information to the virtual machine, use one or more of the options:

```
vmware-fullscreen -poweron [-s variable=value] [-name=<alias>]
                           [-directkey=<keyspec>] [-fullscreen] "<config_file>"
```

When you use these optional switches, the `-poweron` switch is required and must be the first switch after the `vmware-fullscreen` command. Provide the full path to the virtual machine's configuration (.vmx) file at the end of the command line. Enter the complete command on one line.

Use the following optional switches to:

- a `-s` — Pass a variable name and value to be used in configuring the virtual machine. You can include multiple `<variable>=<value>` pairs in the command. Each `<variable>=<value>` pair must be preceded by `-s`.
- b `-name=<alias>` — Give a name to the virtual machine. You can use that alias in `-switchto` and `-poweroff` commands.
- c `-directkey=<keyspec>` — Specify the virtual machine's direct-switch key. If a direct-switch key is specified in the virtual machine's configuration file, the command line overrides the configuration file.
- d `-fullscreen` without `-poweron` — Start a virtual machine and go straight to full screen switch mode. The virtual machine takes over the display immediately, instead of running invisibly until the user switches to it later.
- e (Optional) To start a virtual machine and specify that its direct-switch key combination is Ctrl+Shift+F1, enter the following command on one line:

```
vmware-fullscreen -poweron -directkey=0x70,0x6 "<config-file>"
```

Stop a Virtual Machine

To stop a virtual machine

- Use either of the following commands to stop the specified virtual machine:

- `vmware-fullscreen -poweroff "<config_file>"`
- `vmware-fullscreen -poweroff <alias>`

You can specify the path to the configuration (.vmx) file, or you can specify the alias if you used `-name=` when you started the virtual machine.

Stop All Virtual Machines

To stop all virtual machines

- Use the following command to stop all virtual machines cleanly:

```
vmware-fullscreen -exit
```

Workstation exits when all the virtual machines are powered off.

Switch Among Virtual Machines and the Host

Several commands are available to switch among virtual machines and the host. Depending on which command you use, you can switch to the specified virtual machine, to the host operating system, or to the next machine (virtual machine or host) in the cycling order. A virtual machine must be powered on before you can switch to it. When specifying a virtual machine, you can specify the path to the configuration (.vmx) file, or you can specify the alias if you used `-name=` when you started the virtual machine.

To switch among virtual machines and the host

- Use one of the following commands to switch to the specified virtual machine:

- `vmware-fullscreen -switchto "<config-file>"`
- `vmware-fullscreen -switchto <alias>`
- `vmware-fullscreen -switchto host`
- `vmware-fullscreen -switchto next`

Check the Status of VMware Workstation

To check the status of VMware Workstation

- Use the following command to determine if Workstation is running in full-screen switch mode:

```
vmware-fullscreen -query
```

If Workstation is in full-screen switch mode, the response to this command also reports its process ID and window handle.

List All the Virtual Machines Currently Powered On

To list all the virtual machines currently powered on

- Use the following command to list all virtual machines that are currently powered on:

```
vmware-fullscreen -listvms
```

The list is added to the `vmware-fullscreen` log file.

vmware-fullscreen Log File

The `vmware-fullscreen` program writes to a log file. This log file records errors reported by `vmware-fullscreen` itself as it starts, stops, and passes other commands to Workstation. It is separate from the `vmware.log` file, which stores information on the running virtual machines.

The name of the `vmware-fullscreen` log file is `vmware-
<username>-<pid>.log`. By default, the `vmware-fullscreen` log file is in the `temp` directory for the user logged on to the host computer. This location might be specified in the `TEMP` environment variable. The default location is:

```
C:\Documents and Settings\<username>\Local Settings\Temp
```

The administrator can specify a different location for this log file by adding the following line to the Workstation global configuration file (`config.ini`):

```
fullScreenSwitch.log.filename="<path>"
```

VMware recommends using a full path. If you use a relative path, the location is relative to the directory that is active when the `vmware-fullscreen` command is issued for the first time after the host computer reboots.

Guest ACPI S1 Sleep

Workstation provides experimental support for guest operating system ACPI S1 sleep. Not all guest operating systems support this feature. Common guest operating system interfaces for entering standby are supported.

By default, ACPI S1 sleep is implemented in Workstation as suspend. You can use the Workstation **Resume** button to wake the guest.

With the following entry in the configuration (.vmx) file for a virtual machine, ACPI S1 sleep is instead implemented as power-on suspend:

```
chipset.onlineStandby = TRUE
```

The guest operating system is not fully powered down. You can awaken the virtual machine in the following ways:

- Keyboard input
- Mouse input
- Programming the CMOS external timer

This feature can be useful for test and development scenarios.

BETA

Learning the Basics of ACE

20

This chapter provides an overview of how to use Workstation to create and deploy virtual machines for end users. This chapter includes the following topics:

- [“Benefits of Using VMware ACE”](#) on page 367
- [“Network and Disk Space Requirements for the Administrative Workstation”](#) on page 369
- [“Overview of Creating and Deploying ACE Packages”](#) on page 370
- [“Overview of the ACE User Interface”](#) on page 371
- [“Troubleshooting Users’ Problems”](#) on page 372

Benefits of Using VMware ACE

VMware ACE is a software solution that enables organizations to deploy and manage secure, platform-independent virtual machines that end users can use on their work PC, personal computer, or even a portable USB media device. End users can be either connected to or disconnected from the enterprise network.

VMware ACE enables safe access to enterprise resources from assured computing environments. These isolated PC environments run on top of existing PCs. The assured computing environment (ACE) contains an operating system, enterprise applications, and preconfigured security settings.

With virtual rights management, built-in copy protection controls, and automatic encryption, VMware ACE helps prevent theft, tampering, and unauthorized copying of applications, data, system settings, and files. Administrators can protect data and ensure compliance with IT policies, including software life-cycle management and access to data and applications.

Key Features of VMware ACE

The following sections describe the key features of VMware ACE.

Manageability

- Create standardized hardware-independent PC environments and deploy them to any PC throughout the extended enterprise.
- The virtual rights management interface controls the virtual machine's life cycle, security settings, network settings, system configuration, and user interface capabilities.
- Track instances through the user interface. View and manage the activation, expiration, and other policies of instances managed with ACE Management Server.

Security

- Rules-based network access lets you identify and quarantine unauthorized or out-of-date ACE instances. Enable access to the network once the ACE instance complies with IT policies.
- Tamper-resistant computing environment protects the entire ACE instance and package, including data and system configuration, with seamless encryption.
- Copy-protected computing environment prevents users from copying enterprise information.
- Roles-based SSL communications provides a secure protocol between the ACE Management Server and client.
- Resource signing lets you specify that ACE Resource files be protected from all tampering.

Usability

- The customizable interface lets you customize the behavior and look and feel for users.
- The flexible computing environment lets users revert to a previous state within seconds and can work online or when disconnected from the enterprise network.

VMware ACE Terminology

The following terms are used frequently in the chapters describing VMware ACE features:

- **ACE-enabled virtual machine** – A virtual machine template that the ACE administrator creates. The ACE-enabled virtual machine can be configured with various policies, devices, and deployment settings and then used as the basis for creating any number of packages to be sent to ACE users.
 - **ACE instance** – The virtual machine that ACE administrators create, associate with virtual rights management (VRM) policies, and package for deployment to users. An ACE instance that is managed by an ACE Management Server is a managed ACE instance. An ACE instance that is not managed by an ACE Management Server is a standalone ACE instance.
 - (Optional) **ACE Management Server** – The ACE Management Server enables you to manage ACE instances, to publish policy changes to dynamically update those instances, and to test and deploy packages more easily. Adds new integration with Active Directory setups and provides secure Active Directory and LDAP integration, with role-based secure SSL communication.
- For more information, see the *VMware ACE Management Server User's Guide*.
- **Pocket ACE** – Enables an administrator to bundle and deploy an ACE onto a USB portable media device, including USB flash drives, Apple iPod mobile digital devices, and portable hard drives.

Network and Disk Space Requirements for the Administrative Workstation

As an administrator, you use Workstation to create and manage the virtual machines you distribute to end users. Following is a list of prerequisites for the machine that hosts Workstation:

- If your company already has a library of standard virtual machines, you need network access to that library from your host computer.
 - If you are creating virtual machines, you need access to installers for the guest operating systems and application software that you plan to install in the virtual machines.
- You can install operating systems from CDs, ISO image files on a local drive or on the network, or a PXE server. You can install application software from CDs or installers on a local drive or on the network.
- You need to provide adequate disk space for virtual machine files and package files. The files for each virtual machine can be as large as several gigabytes. The package files can also be large. The default location for the package files is the `Packages` folder inside the virtual machine's folder.

- Workstation needs a substantial amount of temporary working space when it creates a package. The total disk space required is about twice the combined sizes of all the components of the package. The New Package wizard displays information about the amount of space needed and the locations where the space is needed.

Overview of Creating and Deploying ACE Packages

This section provides an overview of the tasks you must perform to create, deploy, and manage ACE instances.

- 1 Create or clone a virtual machine that meets the requirements of your end users.
The procedures are the same as for any virtual machine. For the network type, VMware recommends using Network Address Translation (NAT) or bridged networking with an IP address a DHCP server provides.
- 2 Display the summary tab for the virtual machine and click **Enable ACE Features** in the **Commands** list.
ACE-specific commands are added to the **Commands** list on the summary tab, and the **VM > ACE** menu is enabled.
- 3 Use the **VM > Settings** menu to configure the virtual machine.
(Optional) Use the ACE Options settings panel to associate the virtual machine with an ACE Management Server. You can then use the server to activate and track instances and make changes to policies, instance customization data, and other data for each ACE instance.
Because managed ACE instances check periodically for updates, the updates are dynamic. You do not need to create and deploy new update packages. See the *VMware ACE Management Server User's Guide*.
- 4 Install a guest operating system, VMware Tools, and other software in the virtual machine.
The procedures are the same as for any virtual machine. See the *VMware Guest Operating System Installation Guide*.
- 5 Set policies for the ACE instance.
Policies control such things as what network access end users have from ACE instances and what devices on their host computers they may use in the instances. See [Chapter 21, "Setting and Using Policies and Customizing VMware Player,"](#) on page 373.
- 6 Specify deployment settings for the ACE instance.

Deployment settings control such things as encryption, expiration date, and security IDs. See [Chapter 22, “Deploying ACE Instances,”](#) on page 413.

- 7 Create packages to deploy to end users.

Workstation guides you through the process. See [“Creating a Package”](#) on page 426 or [Chapter 23, “Pocket ACE,”](#) on page 435.

- 8 Distribute packages to end users.

Distribute the packages on CD, DVD, or portable media, or make them available on a network. See [“Deploy Packages”](#) on page 433 or [“Deploying the ACE Package on a Portable Device”](#) on page 437.

- 9 Install ACE instances on end users’ machines.

See [“Installing ACE Instances”](#) on page 441 or [“Run the Pocket ACE Instance”](#) on page 439.

You can install multiple ACE instances on the same machine. They can be from different vendors and be governed by different policies. You can also uninstall individual ACE instances or Workstation while leaving other ACE instances installed.

- 10 Keep users up-to-date.

If you need to update the guest operating system, update a program running inside the ACE instance, or change policies set for the ACE package, you can create and distribute a new package.

Overview of the ACE User Interface

Use any of the following methods to access the policy editor, deployment settings editor, and packaging wizards:

- Select the ACE-enabled virtual machine and choose a command from the **VM > ACE** menu.
- In the summary view for the ACE-enabled virtual machine, click an ACE-related command in the **Commands** list.

The **ACE** tab in the summary view lists the current settings for policies and deployment.

- Click a button in the **ACE** toolbar.
- Right-click the ACE-enabled virtual machine in the sidebar and choose an ACE-related command.

ACE Management Server has two interfaces:

- In Workstation, select an ACE Management Server in the sidebar to display the instance view.
- Use the VMware Help Desk application. Because this interface is browser-based, you can use it from machines that do not have Workstation installed.

Both interfaces offer the same functionality. Administrators can view and control all managed ACE instances. An advanced search function allows you to locate instances in the database quickly. You can customize the interface by adding searchable custom fields. See the *VMware ACE Management Server User's Guide*.

Troubleshooting Users' Problems

End users might need help with lost passwords, expired ACE instances, or copy-protected ACE instances that they have moved to a different location.

Use one of the following methods to fix those problems:

- **Managed ACE instances** – Use ACE Management Server. See the *VMware ACE Management Server User's Guide*.
- **Standalone ACE instances** – Use the `vmware-acetool` command-line program to fix those problems directly on the users' machines. See [“ACE Tools: vmware-acetool Command-Line Tool”](#) on page 450.

You can also use the hot-fix feature to respond to these problems. See [“Setting Hot Fix Policies for Standalone ACE Instances”](#) on page 400 and [“Respond to Hot Fix Requests”](#) on page 452.

You might find it useful to modify the configuration of an ACE instance on an end-user's computer. Administrator mode enables you to access and use the virtual machine settings editor when running the ACE instance with VMware Player on the user's computer. See [“Setting Administrator Mode Policies”](#) on page 399.

Setting and Using Policies and Customizing VMware Player

21

This chapter describes how to set policies for an ACE-enabled virtual machine and customize the VMware Player interface for end users. This chapter includes the following topics:

- [“Benefits of Using Policies”](#) on page 374
- [“Set Policies for ACE Instances”](#) on page 374
- [“Setting Access Control Policies”](#) on page 374
- [“Setting Host to Guest Data Script Policies”](#) on page 382
- [“Setting Expiration Policies”](#) on page 382
- [“Setting Copy Protection Policies”](#) on page 383
- [“Setting Resource Signing Policies”](#) on page 383
- [“Setting Network Access Policies”](#) on page 384
- [“Setting Removable Devices Policies”](#) on page 392
- [“Setting USB Device Policies”](#) on page 393
- [“Setting Virtual Printer Policies”](#) on page 395
- [“Setting Runtime Preferences Policies”](#) on page 395
- [“Setting Snapshot Policies”](#) on page 398
- [“Setting Administrator Mode Policies”](#) on page 399
- [“Setting Hot Fix Policies for Standalone ACE Instances”](#) on page 400
- [“Setting the Policy Update Frequency for Managed ACE Instances”](#) on page 400
- [“Control Which ACE Instances Run on a Host”](#) on page 401
- [“Writing Plug-In Policy Scripts”](#) on page 402
- [“Customizing the VMware Player Interface on Windows Hosts Only”](#) on page 407

Benefits of Using Policies

Policies give you control over many aspects of the ACE instances you distribute to end users. For example, you can set policies for the following security purposes:

- Permit the ACE instance to be used only by certain users and groups defined in an Active Directory domain.
- Specify which network resources end users may access from the virtual machine.
- Permit users to connect and disconnect certain removable devices configured for the virtual machine.
- Set an expiration date for an ACE instance.

You set policies with the policy editor.

You can change some or all of the policies for an ACE instance at any time by editing the policies and creating and distributing a new package that contains only the policies.

For ACE-enabled virtual machines that ACE Management Server manages, you can dynamically change some policies and deploy those changes to the ACE instances on users' machines.

Set Policies for ACE Instances

Policy settings relate to security settings for daily use of ACE instances. For information about encryption settings, see [“Edit Deployment Settings”](#) on page 413.

Before you can use the policy editor on a virtual machine, you must enable ACE features for that virtual machine. See [“Overview of Creating and Deploying ACE Packages”](#) on page 370.

To set policies for ACE instances

- 1 Select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
- 2 In the policy editor, select an item in the **Policy** list.
- 3 Complete the settings panel for that policy and either click **OK** or select another policy to edit.

For assistance with the fields on a settings panel, click **Help**.

Setting Access Control Policies

Activation and authentication policies control access to installed ACE packages and the instances created from those packages. The activation policy specifies who can access

an installed ACE package and turn it into an ACE instance. The authentication policy specifies who can run an ACE instance.

The settings you choose for these policies determine the default settings for package and encryption policies, which protect the ACE packages and files in transit. See [“Encryption Settings”](#) on page 414.

The settings for these policies and how they are implemented vary depending on how your ACE instances are managed and (optionally) tracked. The possible management setups are:

- **Server, with Active Directory** – ACE instances are managed by an ACE Management Server, and the server is integrated with Active Directory.

An end user must enter Active Directory user credentials each time the ACE instance is run. Only the user who activates the instance can authenticate (run) the instance. The activation step is performed whenever an ACE package is installed.

- **Server, no Active Directory** – ACE instances are managed by an ACE Management Server, and the server is not integrated with Active Directory.

The administrator chooses whether the end user must enter a password to activate the ACE instance and run it.

- **Standalone** – ACE instances are standalone, which means they are not managed by a server.

The administrator chooses whether the end user must enter a password to activate the ACE instance and run it.

If you use ACE Management Server, the server also verifies the following items before the instance is allowed to run:

- The revocation flag is not set and the instance is not blocked from running because of any policy errors.
- The expiration date set for the instance, if any, has not been reached. See [“Setting Expiration Policies”](#) on page 382.

Create or Edit an Access Control Policy

After you enable ACE features for a virtual machine, you can create a policy to control which end users can access an installed ACE package and turn it into an ACE instance. This policy also controls which users can power on an ACE instance.

To create or edit an access control policy

- 1 Select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
- 2 In the policy editor, select **Access Control** and complete the fields in the settings panel.
- 3 Click **OK**.
- 4 Verify that the new settings appear correctly on the **ACE** tab in the virtual machine's summary view.

If you change an activation setting, the policy takes effect when a new instance from this package is installed and activated. You can also edit an imported keyword list.

- 5 (Optional) To change the authentication setting from one type to another, create a policy update package and distribute it to the user.

Activation Settings

Use activation settings to control which users can activate an ACE instance after it is installed. The activation date is used for the expiration policy.

If you use an ACE Management Server with Active Directory, the controls in the **Activation** section enable you to open the Active Directory Users and Groups dialog box. The machine on which Workstation runs must be in the same domain that the ACE Management Server is configured for. User-list changes are effective at the next startup of the instance.

If you do not use Active Directory or if you are creating standalone ACE instances, the settings panel includes the following options for activation passwords or keys:

- **None** – No password or key is required. Any user can activate this instance.
- **Password** – The user must enter the password that the administrator uses to activate this ACE instance. You must provide the user with the password through email or other means.

For standalone ACE-enabled virtual machines, you set the password during the packaging process.

- **Activation key** – This option is available if you use ACE Management Server without Active Directory integration. You specify one or more keys and the end user must enter a key that is in that list.

Activation keys are serial numbers (free-form strings) that can be tracked as used or unused by the server. You can enter the keys or import them from a text file.

To import keys, you need a text file that contains the list of activation tokens. Each token is one line in the file. Blank lines are ignored.

After an ACE instance is activated using a key, that key cannot be used to activate another instance. Removing a key from the list does not affect an instance that was activated with that key.

Authentication Settings

The authentication step is performed whenever the user runs the instance, unless **Authentication** is set to **None**.

If you use an ACE Management Server with Active Directory, the controls in the **Authentication** section enable you to open the Active Directory Users and Groups dialog box. The machine on which Workstation runs must be in the same domain that the ACE Management Server is configured for.

If you do not use Active Directory or if you are creating standalone ACE instances, the settings panel includes the following options for authentication control:

- **None** – No password is required. Any user can run this instance after it is activated.
- **User-specified password** – The instance does not run until the user enters the correct password. Each user must set a password during activation, the first time the instance is powered on.

You can create password policies to control such things as the minimum number of characters, types of characters, and number of password attempts before the user is locked out for a specified amount of time.

- **Script** – A custom authentication script is run to determine who can use the instance. See [“Create and Deploy an Authentication Script”](#) on page 377.

Create and Deploy an Authentication Script

You can create a custom authentication script that runs on the end user’s computer to determine who can use the instance.

To require that the script be signed before deployment to prevent tampering, set a resource signing policy. See [“Setting Resource Signing Policies”](#) on page 383.

To provide this script in packages created with an ACE-enabled virtual machine

- 1 Create the script and save it in the ACE Resources directory inside the virtual machine's directory.
- 2 In Workstation, select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
- 3 In the policy editor, select **Access Control** and in the **Authentication** section, click **Set**.
- 4 In the Set Authentication Script dialog box, browse to the script file and click **Open**.
If the deployment platform setting in the deployment settings editor is set to **Both Windows and Linux**, this dialog box contains text fields for both Windows and Linux.
- 5 Type the command for running the script.
Include the script file in the command line, as well as any needed executable file for running the script and any arguments to the script.
- 6 (Optional) Select **Timeout** and type a timeout interval in seconds, in case the script does not run to completion.
The user is denied access if the timeout interval elapses before the script runs to completion.
- 7 Click **OK**.
- 8 If you are enabling this script for an ACE-enabled virtual machine that you already deployed, do one of the following:
 - For standalone instances, include the script in the update package you distribute to end users.
 - For managed instances, use a policy and server update package or a custom package that includes the ACE Resources directory to provide end users with the script.

Include a Power-On and Power-Off Script in the Package

You can provide a script that runs when an ACE instance powers on that determines whether the ACE instance can be run. You can provide a script that runs when an ACE instance powers off to reset any changes made to the host from a power-on script, reset authentication settings, or perform other procedures as the instance powers off.

To require that the script be signed before deployment to prevent tampering, set a resource signing policy. See [“Setting Resource Signing Policies”](#) on page 383.

The power-on or power-off script provides a customizable way of controlling access to an ACE instance in addition to the authentication policy.

To include a power-on and power-off script in the package

- 1 Create the script and save it in the ACE Resources folder.
- 2 On the access control policy page, click **Power-on/off scripts**.
- 3 Do one of the following:
 - Select **Use power-on script to set a power-on script**.
 - Select **Use power-off script to set a power-off script**.
- 4 Click **Set**.
- 5 In the Set Custom Script dialog box, specify the path to the script and enter the command for running the script.
- 6 If you are enabling a power-on or power-off script after you already deployed packages, provide an update package or a custom package with the ACE Resources directory.

When the script runs on the user's system, the script prints "TRUE" for power on or "FALSE" for power off. It must also conform to standard script exit code rules.

The following is an example of a power-on script:

```
#
# VMware Sample Script
#
# Sample script for ACE power-on hook
#
# Description:
# This sample script implements a power-on hook for ACE. This can be used
# in addition to authentication to control the circumstances under which an
# ACE is allowed to run.
#
# This script assumes that the username is defined in the environment
# variable TEST_USERNAME (a fictitious environment variable used for this
# sample) and returns TRUE if the user is allowed to run, and FALSE
# otherwise.
#
# Input to script:
# None.
#
# Returns:
# TRUE if username is on white list.
# FALSE if username is not on white list or is undefined.
#
```

```

# Expected output:
# One of the strings "TRUE" or "FALSE"
#
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
    print "FALSE";
    exit(0);
}

my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
    print "TRUE";
    exit(0);
}

print "FALSE";
exit(0);

```

Scripts can be in any language. For example, you can use a .bat file on Windows operating systems or perl or sh on Linux operating systems. A script provides Workstation with a command-line executable file or a script file in the ACE Resources directory. The guidelines a script must follow depend on which policy the script is implementing.

The script must exit with a 0 (zero) value to be considered a success. Any other output results in failure. Upon success, the stdout output of the script is examined. For a given policy, this should be a specific value such as TRUE or FALSE. For a power-on script, output should be TRUE or FALSE. The authentication script output is used as a password. The host to guest data script is a string in a particular format such as `guestinfo.var1="value1"\nguestinfo.var2="value2"`.

Set a Recovery Key for Encrypted ACE Instances

You can specify the key to be used for access to encrypted ACE instances. This key enables you to reset the password for a deployed ACE instance.

To set a recovery key for encrypted ACE instances

- 1 On the access control policy page, click **Set recovery key**.
- 2 In the Recovery Key dialog box, select **Use recovery key**.
- 3 Do one of the following:

- To use an existing PEM-format key pair, click **Browse for Existing Key** and navigate to the public key of the pair to use.
 - To create a PEM-format key pair, click **Create New Recovery Key** and complete the dialog box that appears.
- 4 Click **OK** to generate the keys.

After several seconds, the newly generated public key is listed in the field on the **Recovery Key** tab. The two parts of the key are stored in the location you indicated, with the names you specified followed by the extensions `.pub` for the public key and `.priv` for the private key.
 - 5 Record the private key password and location of the private key file so that you can supply it if you need to reset a password.

Set Activation Limit

The activation limit is the maximum number of ACE instances that can be activated from the specified ACE-enabled virtual machine.

To set an activation limit

Under **Activation limit**, in **Total number of activations**, choose how many instances can be activated from this ACE-enabled virtual machine.

You can use the drop-down list or type in a number.

Active Directory Password Change Proxying

You can provide additional security for your ACE instances by integrating with Active Directory.

You can specify password expiration and change requirements, set up the domain to expire passwords, and require password changes periodically. These settings are in addition to ACE access control policy settings.

In cases in which Active Directory users need to change their passwords, you can configure the ACE Management Server as an Active Directory password change proxy. In this mode, the ACE Management Server makes the password change request to the Active Directory domain controller on the user's behalf.

Setting Host to Guest Data Script Policies

You can provide a host to guest data script that runs when the ACE instance is powered on or passes values to the guest. Use this policy setting to share specific host information with the guest operating system when the ACE instance is powered on.

The script, which runs on the host, should output a set of key-value pairs, which become available to the applications that are running inside the guest. The VMware Tools service provides this ability. The set of acceptable keys consists of `machine.id` and keys prefixed with `guestinfo`, such as `guestinfo.ipAddress`.

If the ACE-enabled virtual machine for this instance is configured for both Windows and Linux platforms, you can provide scripts for both Windows and Linux systems.

Changes to a script require that you deploy an update package that includes the new script.

Setting Expiration Policies

Expiration policies are useful, for instance if you want to prevent a contract employee from using a virtual machine past a certain date or for more than a certain number of days.

When an instance expires, the files remain on the user's computer, but the instance cannot be used. This way, the user can request an extension to the expiration date.

If you specify a date range, the instance can be powered on and run no earlier or later than the start and end dates. You can deploy ACE instances with expired date ranges.

You can also set and customize a warning message that appears each time an instance powers on as the expiration date approaches. An expiration message appears when the instance expires and the instance can no longer be powered on.

A standalone ACE instance has the same expiration policy as all instances created from the corresponding ACE package. The fixed expiration date or the fixed date range is established at activation time. Each time the user powers on the instance, the date or date range is checked. Expiration checks are also performed while the instance is running. If the expiration is reached, an expiration message appears and the instance is suspended.

With a managed ACE instance, the expiration policy works similarly as for standalone instances, but the expiration policy value can be specified for individual instances. A valid date range for an ACE-enabled virtual machine applies to each of its associated ACE instances until an instance is individually configured with its own date range. After that configuration, any changes to the ACE-enabled virtual machine's expiration

policy do not affect the instance. All expiration values, both for ACE-enabled virtual machines and for all ACE instances, are dynamic.

Setting Copy Protection Policies

Copy protection policies ensure that an ACE instance runs only from the location where it was originally installed. If you copy-protect an ACE instance, its files can be moved or copied, but the instance cannot run from the new location.

For standalone ACE instances, you can specify whether copying and moving are allowed. For managed ACE instances, you can specify whether both copying and moving are allowed or whether only moving is allowed. In this case, only one copy of the ACE instance is allowed to run at a time.

If the user moves or copies a copy-protected ACE instance and tries to run it, an error message appears. It lists an alphanumeric string that the user can send to the system administrator or help desk assistant to get the copy protection changed.

For managed instances, you can also dynamically change the copy protection settings, switching the settings so that moved or copied instances will run or not run.

Every ACE instance has a copy protection identifier (CPID) that contains the path to the ACE instance on the host file system. For standard ACE instances, the CPID also contains the system's BIOS ID. For Pocket ACE instances, the CPID contains the file system ID. If copy protection is on, Workstation compares the current CPID with the stored CPID. If they do not match, the instance was moved or copied.

For standalone ACE instances, you can set the CPID by using `vmware-acetool` or by sending hot-fixes (on Windows systems, if hot-fixes are enabled). See [“ACE Tools: vmware-acetool Command-Line Tool”](#) on page 450 and [“Respond to Hot Fix Requests”](#) on page 452.

For managed ACE instances, the CPID is stored on the server and the administrator can update it. See the *ACE Management Server User's Guide*.

Setting Resource Signing Policies

You can set the resource signing policy so that an ACE instance cannot be run if resource files, such as policy scripts or custom EULA text files, are tampered with.

A resource is considered any file in the ACE `Resources` subdirectory in the virtual machine directory on the Workstation host. Files that are put in this directory on the end user's machine are not resources in this sense and are not signature checked.

Signature checking is performed on the end user's machine at power on and then every time a script is run. You can specify whether to verify all files in the ACE **Resources** directory or just the policy scripts in that directory.

If you are creating a package that has substantial resources, such as large files or large numbers of files, signature checking might take a long time. In this case, consider verifying scripts only or not using resource signing.

NOTE If you set the encryption package setting options to **None**, any verification specified in the resource signing policy is not performed. The encryption package setting overrides the resource signing policy. See [“Encryption Settings”](#) on page 414.

Setting Network Access Policies

The network access feature uses a packet-filtering firewall to enable you to specify which machines or subnets an ACE instance or its host system may access. This means that you can, for example, configure the instance so that it is allowed to connect only to your VPN server, which then controls access to other resources.

You can also customize the network access settings to filter on the basis of network addresses, traffic direction, protocol, and ports. You can set the following types of network access restriction definitions:

- Network zones
- Network access for the ACE instance's host machine (also known as “host network access”)
- Network access for your ACE instance's guest operating system (also known as “guest network access”)

Network access policies can be dynamic if the ACE instance is associated with an ACE Management Server. This means, for example, that you can quickly lock ACE instances out of all or part of your network to help combat the spread of a worm or virus without deploying updated packages. See the *VMware ACE Management Server User's Guide*.

Before You Begin Setting Host Policies

Use the following guidelines as you plan network access policies:

- A host machine for ACE instances can have only one host policy file. If you try to install an ACE package with a host policy file on a machine that already has a different host policy file, installation of the new package fails.



CAUTION Host policy settings might conflict with settings in certain other software running on the host computer, such as software firewalls. For information on configuring software on the host computer to avoid these conflicts, see the technical note “VMware ACE Technical Note - Host Software and Advanced Network Quarantine.”

- A host policy is in effect even when no ACE instances are running. The policy starts immediately after installation and starts working every time the host system boots.
- Any restrictions on the host’s network access also restrict network access for an ACE instance that uses NAT networking, because the NAT connection is affected by all the policies you apply to the host. If you set up restricted host access by using the ruleset and rules editors rather than the Network Access wizard, configure the ACE-enabled virtual machine’s virtual NICs to use bridged networking.
- If you are setting up a managed ACE-enabled virtual machine, you must allow the host to access the ACE Management Server, communicating through TCP over the appropriate port that you configure.
- Host policies do not apply to Pocket ACE instances. If you specify a restricted host policy for an ACE-enabled virtual machine and then attempt to create a Pocket ACE package with that ACE-enabled virtual machine, the package is created but the host policy is not included in the package.
- You cannot view changes to host policies in the preview mode. If you want to test the effects of such changes, you must perform a test deployment. See [Chapter 22, “Deploying ACE Instances,”](#) on page 413.

Use the Network Access Wizard to Configure Network Access

VMware recommends that you use the Network Access wizard to configure basic settings and then use the zone and ruleset editors to fine-tune the settings if necessary.

The Network Access wizard creates or changes rules for the following zones:

- If you choose the **Desktop Configuration** option, the wizard creates a new guest access ruleset for the Everywhere zone. This ruleset restricts ACE instance access to your VPN or other specified network hosts.
- If you choose the **Laptop Configuration** option, the wizard creates a new internal zone that restricts the network address and, optionally, the domain on which the ACE instance can run. It can also create a new host access ruleset for this zone to restrict access to the internal network. For example, you can specify a proxy server.

Finally, you can configure the same remote access as for the **Desktop Configuration** option.

If you use this option and you do not modify any of the default settings that the wizard provides, the host is still allowed to communicate with DNS and DHCP servers so that the zone-detection mechanism can function properly.

To use the Network Access wizard to configure network access

- 1 In the policy editor, select **Network Access**.
- 2 Select **Restrict network access of the ACE instance and its host** and click **Quick Setup**.
- 3 Complete the wizard.

Depending on which configuration type you choose, a new zone might be added to the Network Access settings panel, and new rulesets might appear in the **Host Network Access** and **Guest Network Access** columns in the table.

- 4 (Optional) To view or edit the zones or rulesets you created with the wizard, click the zone or ruleset name in the table on the Network Access settings panel.

When you use the Network Access wizard to create an internal zone, choosing the **Laptop Configuration** option enables you to specify the network address, domain, and subdomains. If you want to also configure DNS, DHCP, WINS, or gateway servers, use the zone editor. See [“Guidelines for Specifying Zone Conditions”](#) on page 386.

Guidelines for Specifying Zone Conditions

Zone conditions describe the characteristics of a network zone. Workstation examines the networks that are directly connected to network adapters on the host computer to see if a match exists for all the criteria for any adapter in any of the zone definitions.

Details about zone matching are:

- You can specify a zone by using up to six conditions:
 - Domain
 - Subnet
 - DNS servers
 - DHCP servers
 - Gateway servers
 - WINS servers

For a match to occur, all specified conditions must be met.

- All zone conditions except the domain condition allow users to specify a list of addresses. The match is made if the host's address matches any of the address-list entries in a specified condition.

When the host connects to a network, a check is performed to determine whether the network matches the conditions for a zone. The checking starts with the topmost zone in the table and continues down the table until a match is made or the Everywhere Else zone is reached. When a match is made, the zone checking stops and filter rules for that zone are applied.

There are trade-offs between using shorter and longer lists of conditions. If you use a longer list, you minimize the chances of a false-positive result or a misidentification. Minimizing the chance of a false-positive result or a misidentification can be important if you are providing an ACE package to someone who connects a host computer to multiple networks at different times. If one of the other networks matches the characteristics you define in the zone definition, the host and instance access policies are applied, even if the host is not connected to your network.

In some cases, however, using a longer list might also increase the likelihood that a user could circumvent the detection mechanism. For example, such an error might be made if you switch the host to use a static IP address instead of DHCP and configure the host with only a subset of the characteristics defined for your zone, such as only network address, or network address and DNS server information.

Also consider that the addresses or names of certain servers can change over time. Such changes can also introduce detection issues.

Using a smaller set of information in a zone description, such as only the network address and the subnet mask, is safer. The disadvantage is that it increases the chance that a false positive or misidentification can occur. Such false positives are especially likely if your network is using a common netblock, such as 10/8, 172.16/12, or 192.168/16, that is also used by other networks.

Descriptions of the Zone Condition Settings

Each zone description must contain one or more of the following setting options describing the conditions of the zone:

- **Domain** – Specifies the domain name of the network, such as `mycompany.com`. Enter only one domain name. The value of **Allow subdomains of this domain** governs the interpretation of this option.
- **Allow subdomains of this domain** – Modifies the **Domain** option. It specifies whether, for the **Domain** zone condition to be met, a domain name must exactly match the domain name specified in the **Domain** box or whether a match of the domain name is made any time the string contains `<domain_name>`. For example,

if this option is selected, `corp.mycompany.com` is considered a match for `mycompany.com`. If this option is not selected, `corp.mycompany.com` is not considered a match for `mycompany.com`.

- **Network address** – Specifies an IP address or subnet range that the network uses. The value of `<subnet>`, if you include a subnet range, must be the number of bits in the netmask. A network adapter matches this condition if it is using an IP address that lies within any of the specified ranges.
- **DNS servers** – Specifies one or more IP addresses or host names for DNS servers on the network. A network adapter matches this condition if it is using at least one of these servers.

If the value of the **Match at least** option is greater than 1, the host must be using the specified number of DNS servers on the list before a network adapter is considered to be on the defined network.

Because multiple methods exist for assigning DNS domain names to a Linux host, using just the DNS domain name to define a zone can be error prone. To define a zone for a Linux host, use criteria in addition to the DNS domain names.

- **DHCP servers** – Specifies one or more IP addresses or host names for DHCP servers on the network. A network adapter matches this condition if it is using at least one of these servers.
- **Gateway servers** – Specifies one or more IP addresses or host names for default gateways on the network. A network adapter matches this condition if it is using at least one of these gateways.
- **WINS servers** – Specifies one or more IP addresses or host names for WINS servers on the network. A network adapter matches this condition if it is using at least one of these servers. Linux hosts ignore WINS server settings during zone detection.

If the value of the **Match at least** option is greater than 1, the host must be using the specified number of WINS servers on the list before a network adapter is considered to be on the defined network.

Add or Edit a Network Zone

Use the zone editor to configure the network address, domain, DNS, DHCP, WINS, or gateway servers that an ACE instance can use for network connections.

Before you open the zone editor, determine what criteria to use for connecting to internal and external networks. See [“Guidelines for Specifying Zone Conditions”](#) on page 386 and [“Descriptions of the Zone Condition Settings”](#) on page 387.

To add or edit a network zone

- 1 In the policy editor, select **Network Access**.
- 2 In the Network Access settings panel, do one of the following:
 - To add a zone, click **Add Zone** and click the **New Zone** entry that appears in the table.
 - To edit a zone, click the name of the zone in the Zones column of the table.
- 3 Complete the fields in the zone editor that appears and click **OK**.

Using the Ruleset Editor to Configure Host and Guest Access

Each access setting for the ACE instance's host machine and for the ACE instance's guest system is based on a set of access rules. Whenever you use the Network Access wizard, a default ruleset is used for host and guest network access. You can use the ruleset editor to change the parameters of those rules.

Network access policies are applied by filtering on the IP address, the protocol number from the IP header, the direction of traffic, and TCP and UDP port values. The filtering does not involve deep packet inspection. For DNS and DHCP access, the TCP and UDP ports on which those services traditionally reside are opened.

Note the following aspects of the filtering actions:

- If you move your services to different ports, the network access rules for those services no longer work.
- The host or instance is open to all traffic on these protocols and ports.

To understand the particulars of how traffic is being blocked or allowed for DNS, DHCP, and ICMP protocols and ports, see the rules displayed in the ruleset editor.

Add or Edit Rulesets and Rules for Network Access

The rules in the ruleset editor are listed in the order in which they are to be evaluated. When a network traffic packet arrives or is to be sent from the host or guest, it is compared with each rule in the ruleset, in order from the top down. If the following packet settings match the rule conditions, the packet is allowed or blocked according to the rule's action:

- Source address for incoming packets
- Destination address for outgoing packets, protocol, and ports

The packet is compared to each rule in order until it matches a rule or it was compared with all of the rules. When a match is made, the packet-to-rule comparison ends. The

packet is not compared to subsequent rules in the ordered list. If it was compared to all rules without a match, the default rule action is applied.

To add and edit rulesets and rules for network access

- 1 In the policy editor, select **Network Access**.
- 2 In the Network Access settings panel, click the link in the table column that applies to the access setting to edit.

The Zone and Access Type information just below the **Ruleset Name** text box shows the name of the zone and whether the access setting applies to host network access or to the network access for ACE instances (guest).

- 3 Use the ruleset editor to change the order of rules in the set, edit rules, and specify whether the host or guest is allowed to use DNS, DHCP, or ICMP.

By default, **DNS**, **DHCP**, and **ICMP** are included in the network access setup for both host and instance access. VMware recommends that you keep **DHCP** and **DNS** selected because they are important for zone detection.

Whether the following settings apply to the host or to the ACE instance (guest) depends on whether you are editing a host network access ruleset or a guest network access ruleset:

- **DNS** – Allows the guest or host to use a DNS server to resolve IP addresses. Select this option if the DNS server is not included in any other network access setting for this host or ACE instance.
 - **DHCP** – Allows the host or guest to obtain its IP address from a DHCP server. Select this option if the DHCP server is not included in any other network access setting for the host or ACE instance.
 - **ICMP** – Enables you to use the `ping` command. For guests, `ping` enables you to check network connectivity to and from the ACE instance. For hosts, it enables you to check network connectivity with other hosts in the network and with the ACE instance.
- 4 (Optional) To add or edit a rule, do one of the following:
 - To change a specific rule's settings, click the row for that rule in the table in the ruleset editor and click **Edit**.
 - To add a rule, click **Add**.
 - 5 (Optional) Use the rule editor to specify the type of traffic, whether to block or allow traffic from specified network locations, the protocol, and ports or port ranges.

- **Addresses** – To edit an existing host name or address, double-click that item and edit it. The wildcard setting for all IP addresses is 0.0.0.0/0.
- **Protocol** – To allow or block communication for a specific protocol, select **Custom** from the **Protocol** list. The protocol number is in the packet. If that number matches the number supplied in the **Custom** field, the packet is allowed or blocked as the rule specifies. The protocol number is used in the protocol field of IPv4 packets.

For a list of protocol numbers, see the Internet Assigned Numbers Authority (IANA) organization's Web site. Most protocol numbers are permanently assigned.

- **Remote Ports and Local Ports** – If you are using either TCP or UDP and want to qualify the rule with specific port numbers for this type of traffic, type the port numbers or port-number ranges.

The wildcard port setting is "" (double quotation marks).

Usually you specify filtering on either local or remote ports, not both, because both specifications have to match for the rule to be applied. (DHCP represents an exception to this general rule.)

The local port is the source port for outgoing packets and the destination port for incoming packets. Typically you specify a local port when the host or guest is being used as a server obtaining remote connections on some port.

The remote port is the source port for incoming packets and the destination port for outgoing packets. Typically you specify a remote port when the host or guest is a client and is contacting a remote server on some port.

Change NAT Settings

You can use the NAT feature of the network access policy to specify the IP address range for the virtual network VMnet8 on the ACE instance's host system. You deploy this network properties setting with the ACE package.



CAUTION If you set this property, the setting affects all of the ACE instances and virtual machines on this instance's host system.

To change NAT settings

- 1 In the policy editor, select **Network Access**.
- 2 Click **NAT Settings** on the policy page.

- 3 In the NAT Settings dialog box, select **Assign IP addresses from this subnet**.
- 4 Type the subnet IP address to use and enter zero (0) as the last byte in the address, and click **OK**.
- 5 Create an ACE package and deploy the package.

The NAT setting is not a dynamic policy setting. You can change the setting for a deployed ACE instance only by changing it in the policy and then creating and deploying a new ACE package.

Understanding the Interaction of Host and Guest Access Filters With Tunneling Protocols

Host and guest access filters can differ in their interactions with tunneling protocols.

A host network access filter sees traffic before packets are encapsulated in the tunneling protocol (for example, VPN). A guest network access filter sees traffic after the packets are encapsulated in the tunneling protocol.

Because of this guest access filter behavior, a user might be able to circumvent guest access restrictions by using tunneling protocols or proxies.

Updating a Network Access Policy

You must create and deploy a new package in order for the host policy to take effect.

If you use a managed ACE-enabled virtual machine to create packages that do not contain a host policy and later edit the ACE-enabled virtual machine's network access policy to include a host policy and publish the change, instances created from packages of that ACE-enabled virtual machine do not have a host policy applied. A warning appears on the network access policy page if you attempt to apply a host policy in this way.

You can package just the host policy in a custom package, keeping the package size small.

Setting Removable Devices Policies

Removable devices policies allow you to control whether users can connect and disconnect removable devices from their ACE instances.

A removable devices policy is applied to an ACE-enabled virtual machine and affects all users of all instances created from that ACE-enabled virtual machine.

When you select **Removable Devices** in the policy editor, all removable device types for this ACE-enabled virtual machine are displayed in a list. You can specify which devices to allow end users to access.

Setting USB Device Policies

You can set USB device policies to restrict the ACE user's access to USB devices. The policies are dynamic, so you can allow and then block access to USB devices.

Access Levels for USB Devices

You can set restrictions at various levels of specificity, and you can mix levels of restriction in a policy setting. The levels of restriction are:

- **Specific USB device** – For example, allow use of a specific type of digital camera but disallow use of iPod mobile digital devices.

If a rule exists for a specific device, that rule overrides any rules set for device classes in which the device belongs.

All entries in the list of specific USB devices are maintained in a device database that is included with the files for this ACE-enabled virtual machine. You can copy and share the database. It is not write-protected. The default location for the file is

C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation\usbhistory.ini

- **Device class** – For example, allow use of human input devices (HIDs), such as mice and keyboards, but disallow use of communications devices, such as modems and cell phones.

If no specific device rule exists for a device and more than one device class rule applies to that device, the most restrictive rule is applied. For example, a device might include both a fax function and a print function and therefore can belong to more than one class. If one rule blocks a fax device but another rule allows a print device, the combination fax and print device is blocked.

- **All USB devices** – Allow or deny access to all connected USB devices. Device class rules and specific device rules override general access rules.

Set an Access Policy for USB Devices

You might want to set a policy that prevents end users from connecting such USB devices as mass storage devices, printers, or modems to the ACE instance.

Before you use the policy editor, determine a strategy for setting the policy. If you want a restricted environment, you can plan to generally block access to all USB devices and then specify exactly which classes or specific devices to allow. See [“Access Levels for USB Devices”](#) on page 393.

To set an access policy for USB devices

- 1 In the policy editor, select **USB Devices**.
- 2 Use the **General access to all USB devices** radio buttons to specify whether to allow or block general access to USB devices.
- 3 To specify a USB policy by device class:
 - a If the device does not appear in the **Access to specific types of USB devices** list, click **Add**, select the device in the USB Device Classes dialog box, and click **OK**.

You can Ctrl-click and Shift-click items to select more than one class.
 - b Use the **Allow** and **Block** check boxes in the **Access to specific types of USB devices** list to specify the rule for each device in the list.
- 4 To specify a USB policy by specific device:
 - a If the device does not appear in the **Access to individual USB device models** list, click **Add**, select the device in the USB Device List dialog box, and click **OK**.

If the device does not appear in the USB Device List dialog box, do one of the following:
 - Connect the device to the host and click **Refresh**.
 - Determine the device's vendor ID (VID) and product ID (PID) and click **Manual Add** to enter the information. This information is available from the Windows Device Manager when you connect the USB device to a Windows computer.
 - b Use the **Allow** and **Block** check boxes in the **Access to individual USB device models** list to specify the rule for each device in the list.
 - c (Optional) To change the information for a device, click **Remove** and add the device again with the new information.
- 5 Click **OK**.

Setting Virtual Printer Policies

VMware ACE includes a virtual printer that allows users to print to any printer available to the host computer without installing additional drivers in the virtual machine.

The virtual printer feature is available for ACE instances running with these Windows host and guest operating systems:

- Host – Windows 2000, XP, 2003, or Vista, 32-bit only
- Guest – Windows 2000, XP, 2003, Vista (32- and 64-bit), Red Hat Enterprise Linux 4 (32 bit only), Ubuntu, and SUSE

After you enable the virtual printer policy, a serial port is added to the virtual machine. This serial port appears on the **Hardware** tab of the virtual machine settings editor, with the **Used by Virtual Printer** summary. You can only add or remove this serial port by enabling or disabling the option in the virtual printer policy.

NOTE If the ACE-enabled virtual machine already has four serial ports, you cannot add another serial port for the virtual printer. To enable the virtual printer, delete an existing serial port.

After they install the ACE instance, end users can use the **VMware Player > Virtual Printers** menu command to specify which printers from the host are available to the guest. If end users on Windows hosts have problems, make sure the TP AutoConnect Service Windows service is started.

Setting Runtime Preferences Policies

You can set options on the runtime preferences policy page to specify which Workstation runtime attributes the user can choose.

Runtime Preferences Settings

Use the following information to decide which features are enabled:

- **Always run in full screen** – VMware Player fills the full screen when it starts, hiding the host operating system. You might find this useful, for example, to avoid confusion about the differences between the host system environment and that of the ACE instance.

Users can return to the host operating system by clicking the minimize button on the toolbar. If the mouse pointer is not available, pressing Ctrl+Alt minimizes the display.

- **Always hide the full screen toolbar** – End users cannot display the toolbar that usually appears at the top of the screen when in full screen mode.
- **Always run in appliance view** – The ACE instance opens in appliance view and the user cannot change to console view.

To use this setting, you must also enable appliance view for the virtual machine. See [“Set Up Appliance View for a Virtual Machine”](#) on page 169. If you attempt to use this policy without enabling appliance view, an error message appears when the user attempts to start the ACE instance.

- **Do not allow users to modify the memory allocation** – The **Change Memory Allocation** command does not appear in the **VMware Player > Troubleshoot** menu of VMware Player.
- **Reduce virtual machine memory size if needed when powering on** – The virtual machine powers on even if the amount of available memory is less than the amount configured for the virtual machine. If you do not use this feature and the required amount of memory is not available, users need to modify the memory allocation to power on the virtual machine.

Enhanced Virtual Keyboard Settings

Use the following information to decide which features are enabled:

- **Use the enhanced virtual keyboard for secure input** – This setting applies to only to Windows hosts running 32-bit Windows guests, except for Windows Vista guests. This feature provides better handling of international keyboards and keyboards with extra keys. It also provides security improvements because it processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that is not already at a lower layer.

If an ACE instance uses this feature, when end users press Ctrl+Alt+Delete, the guest system only, rather than both guest and host, responds to the command.

Before you create a runtime policy for this feature, turn on the enhanced keyboard filter with the virtual machine settings editor. See [“Use the Enhanced Virtual Keyboard for Windows Hosts”](#) on page 324.

When the ACE instance is installed and the guest operating system starts for the first time, a special keyboard filter driver is installed on the host. After installation, the end user must restart the host computer. Keyboard filtering is then enabled.

- **When a suspected keylogger is detected** – Keystroke logging is a method of recording user keystrokes, including determining user passwords. VMware ACE now includes a keylogger detection feature that can detect keyloggers below

Win32. It cannot detect user-level keyloggers. If you select **Ask user what to do**, end users can exit or continue using the virtual machine if a keylogger is detected. (This feature is experimental in this beta release.)

Exit Behavior Settings

Use the following information to decide which features are enabled:

- **When closing a non-Pocket ACE instance** – If you select **User Preference**, the user has access to **Suspend** and **Power off** in the Preferences dialog box in VMware Player (**VMware Player > Preferences**). If you select one of the other choices, the end user's virtual machine is suspended or powered off when the user chooses **VMware Player > Exit** or clicks the close box in VMware Player.
- **When closing a Pocket ACE instance** – If you select **User Preference**, the user has access to **Go mobile** and **Ask to go mobile or stay connected to the computer** in the Preferences dialog box in VMware Player (**VMware Player > Preferences**).
 - **Always go** – The virtual machine is powered off and synchronized to the host. After synchronization, the user can unplug the USB device and use it in another machine.
 - **Always stay** – The user wants to exit VMware Player but does not want to unplug the device. The virtual machine is suspended and no synchronization occurs.
 - **Always discard** – The user wants to exit VMware Player but does not want to synchronize. All changes are lost.
- **Disable the ability for users to manually power off or reset the virtual machine** – The **Reset** and **Power off and Exit** commands do not appear in the **VMware Player > Troubleshoot** menu. To power off or suspend the ACE instance, the user must exit VMware Player.

Pocket ACE Cache Settings

For performance reasons, when you use Pocket ACE, files from the USB device are cached as needed on the host. When you are finished using the Pocket ACE, you synchronize changes so that the updated files are written to the USB device.

You can disable this caching if you do not have enough disk space on the host. For example, if the virtual disk on the Pocket ACE has 8GB, you might potentially need 8 GB of disk space on the host for caching. You can also disable caching for security reasons if you do not want to create a cache on the host.

If you disable caching, the exit behavior in the **When closing a Pocket ACE instance** list changes to **Always go** but synchronization does not occur because it is not necessary.

Setting Snapshot Policies

You can set policy options for two types of snapshots:

- **Reimage snapshots** – At installation time, a snapshot is taken after all of the required instance setup steps are complete, including, if applicable, encryption, instance customization, and domain join. The snapshot is taken before the virtual machine runs for the first time.

NOTE Manually disable the automatic reimage snapshot by editing the ACE-enabled virtual machine's `aceMaster.dat` file. Edit the `packaging.takeReimageSnapshot` option.

Reimage snapshots allow the ACE administrator, or the user if the administrator enables reimage snapshot options for the user, to revert the ACE instance to its known good starting state or to the known good updated reimage state.

If you enable reimage snapshot options, commands for the options appear in the **VMware Player > Troubleshoot** menu.

If you choose not to enable the reimage snapshot options for the user, you can replace the reimage snapshot or revert to it on the user's machine by providing administrator mode access through the Administrator Mode policy. See [“Setting Administrator Mode Policies”](#) on page 399.

- **User snapshots** – You can enable users to take a snapshot of the ACE instance either when the instance is running or immediately after powering it off. You can also enable them to delete that user snapshot.

User snapshots enable the user to return the virtual machine to a known stable state. User snapshots can be taken, reverted to, and deleted without affecting the reimage snapshot. Only one user snapshot can be saved at a time.

If you enable user snapshot options, commands for the options appear in the **VMware Player > Snapshot** menu.

NOTE You can not take snapshots of a Pocket ACE instance. For more about Pocket ACEs, see [Chapter 23, “Pocket ACE,”](#) on page 435.

Setting Administrator Mode Policies

You can use the administrator mode policy to set an administrative password so that you can do any of the following:

- Run the ACE instance on the user's machine and enter administrator mode to access the virtual machine settings and make changes to the instance's configuration (on Windows systems only). You can only edit the settings. You cannot add or remove virtual hardware devices.
- Run the ACE instance on the user's machine and enter administrative mode to access all the snapshot commands. See [“Setting Snapshot Policies”](#) on page 398.
- Use the `vmware-acetool` command-line program on an ACE user's system to fix a limited set of problems for standalone ACE instances.

Use Administrator Mode on an ACE Instance

Using administrator mode on an end user's virtual machine enables you to troubleshoot and access features and commands that might not be available to the end user.

To use administrator mode on an ACE instance

- 1 Start VMware Player on the end user's machine and choose **VMware Player > Troubleshoot > Enter Administrator Mode**.
- 2 Enter the password for administrator access.
- 3 Choose the appropriate commands as follows:
 - To edit virtual machine settings from the user's machine, choose **VMware Player > Troubleshoot > Virtual Machine Settings**. This command is available only on Windows hosts.
 - To use the user snapshot commands, choose **VMware Player > Snapshot**.
 - To use the reimage snapshot commands, choose **VMware Player > Troubleshoot > Revert to Reimage Snapshot**.
 - To use the ACE Tools, see [“ACE Tools: vmware-acetool Command-Line Tool”](#) on page 450.
- 4 When you finish changing virtual machine settings or using the snapshot commands, choose **VMware Player > Troubleshoot > Exit Administrator Mode**.

Setting Hot Fix Policies for Standalone ACE Instances

This policy enables users of standalone ACE instances to request hot-fixes if they lose or forget the ACE password, try to run an expired ACE instance, or move a copy-protected ACE instance to a new location.

To address these types of problems for managed rather than standalone ACE instances, use the VMware Help Desk Web application or the instance view in Workstation. For more information, see the *ACE Management Server User's Guide*.

The hot-fix request is a file that the user must submit to an administrator for action. You configure whether the user submits the file to an administrator manually or through email generated by the Hot Fix Request wizard.

For automatically generated email, the Hot Fix Request wizard on the user's computer attempts to use a MAPI email client on the host operating system. The hot-fix request file is included as an attachment to the email message. The message uses the email address and subject line that you specify.

If you choose email and the automatic submission fails, the Hot Fix Request wizard allows the user to save the hot-fix request as a file. The user must then send the file to an administrator manually.

The administrator uses Workstation to respond to hot-fix requests. See [“Respond to Hot Fix Requests”](#) on page 452.

Setting the Policy Update Frequency for Managed ACE Instances

This policy controls how often an ACE instance connects to the ACE Management Server to download policy updates while it is running. It also controls how long a managed ACE instance can be used if it cannot connect to the ACE Management Server.

This policy applies only to managed ACE instances. To deploy policy updates for standalone ACE instances, you must create policy update packages. Policy changes are applied when the instance is started after the update package is installed.

The settings for offline usage include text for warning and timeout messages. You can customize messages by adding text to them. You cannot edit the existing standard text except by using the controls on the panel to change the number of minutes, hours, or days shown.

Policy updates take effect while the instance is running, with the following exceptions:

- Updates to access control policies, which include user and group lists, passwords, and scripts, take effect the next time the instance is powered on.

- Updates to policy update frequency policies, if set to **Only when the ACE instance powers on**, take effect the next time the instance is powered on.

Control Which ACE Instances Run on a Host

You can set restrictions such as the following:

- Specify whether virtual machines that are not ACE instances can run on the machine. This is a host-wide policy, which requires an administrator to install the package.
- Specify that only ACE instances with a specific creator ID can run on the machine.

You can control which virtual machines and ACE instances can be run on a host by editing the `aceMaster.dat` file in the virtual machine directory.

To control which ACE instances run on a host

- 1 On the administrator machine where Workstation is installed, power off and close the ACE-enabled virtual machine.
- 2 Use a text editor to open the `aceMaster.dat` file for the ACE-enabled virtual machine.

This file is located in the same directory as the configuration file (`.vmx` file) for the ACE-enabled virtual machine.

- 3 (Optional) To specify that non-ACE virtual machines cannot run on the host, find the `allowVMs` property and change it from 1 to 0.
- 4 Find the `requiredCreatorID` property and set it to an identifier.

For example, to set the required creator ID to `creator1`, edit the line as follows:

```
requiredCreatorID = "creator1"
```

You set `requiredCreatorID` once for each host. You do not need to set this property on other ACE instances that run on the same host.

This is a host-wide policy, which requires an administrator to install the package.

- 5 Find the `creatorID` property and set it to the same identifier.

For example, to set the creator ID to `creator1`, edit the line as follows:

```
creatorID = "creator1"
```

Only ACE instances with this creator ID can run on the same host.

The ID string is in plain text in the `aceMaster.dat` file on the administrator's machine, but it is hidden in the policy file.

If you publish the policy set of an ACE instance to `requiredCreator=yourPolicySetting` and install it on a host, only you (or others with access to the administrator files) know what the creator ID is. Without knowing the `requiredCreator` policy setting, you cannot create your own ACE instance that can run on the host.

6 Do one of the following:

- If you are creating a new ACE instance, create a package for this ACE-enabled virtual machine and install it on the end user's host.
- If you are creating an update for a standalone ACE instance, create an update package.
- If you are creating an update for a managed ACE instance, open the virtual machine and publish the changes to the ACE Management Server.

Changes to the `allowVMs` property or the `requiredCreatorID` property represent changes to host-wide policies. Packages that include these host policies require administrator privileges to install.

Run Multiple ACE Instances on an End User's Machine

To run multiple ACE instances on the end user's machine, determine which ACE-enabled virtual machine you want to use for setting host-wide policies.

To run multiple ACE instances on an end user's machine

- 1 Edit the `aceMaster.dat` file for the other ACE-enabled virtual machines and set the `creatorID` property to the same value that you used in [Step 5](#).

Set only the `creatorID` property and not the `requiredCreatorID` property for these other virtual machines.

- 2 Repeat [Step 6](#).

Writing Plug-In Policy Scripts

You can write scripts to control certain policies in VMware Player. You may use any language that is supported on the user's computer.

For security reasons, scripts must be deployed as part of a package and installed by the package installer. Users cannot modify these scripts.

When scripts run, they must write the appropriate values to the `StdOut` file. Output to the `StdOut` file might be up to 4096 bytes long.

Place any scripts you want to use for a package in the **ACE Resources** directory in the virtual machine directory. Do not place them in a subdirectory of the **ACE Resources** directory. If the scripts need any additional resource files, place those files in the main **ACE Resources** directory. Make sure the script uses relative paths to reference those resources.

Scripts can also write messages to the `StdErr` file. Output to the `StdErr` file may be up to 4096 bytes long. Any messages generated on the `StdErr` file are captured in the log file on the end user's machine at the following location:

```
<UserAppData>\VMware\VMware ACE\<package_name>\Virtual  
Machines\<VM_name>\vmware.log
```

The exit code of a script indicates whether the script succeeded or failed.

[Table 21-1](#) describes the environment variables set in the script execution environment.

Table 21-1. Environment Variables

Variable	Description
VMWARE_MASTER_ID	The ID of the ACE-enabled virtual machine (ACE master).
VMWARE_PACKAGE_ID	The ID of the package the virtual machine was instantiated from.
VMWARE_INSTANCE_ID	A Boolean value that is set to TRUE the first time the virtual machine is powered on. Otherwise, it is set to FALSE.

All scripts run each time the end user starts VMware Player or resets the virtual machine. Some might run more often. For example, an expiration script is run every 24 hours.

The sample scripts presented in [“Sample Policy Scripts”](#) on page 403 are installed with VMware Player in the following location:

```
C:\Program Files\VMware\VMware Player\Samples
```

The topics that follow show the format for the output that your scripts must write to the `StdOut` file to control various policies.

Sample Policy Scripts

The following sections contain sample policy scripts.

Example of an Authentication Script

This script example includes the basic elements required for any authentication script. The purpose of an authentication script is to do one of the following:

- If the user is to be granted access to the virtual machine, generate the data used to create the key for this user and send it as output. The data must be unique for each user. If access is granted, the exit code is 0.
- If the user is to be denied access to the virtual machine, the script exits with a non-zero exit code. This is a reference to the exit code, not the output value.

The output of the script is hashed to create a key to encrypt and decrypt virtual machine files. The first time this script is run, the output is hashed to encrypt the virtual machine. When a virtual machine is decrypted, the script must return the same value. If the script returns a different value, the virtual machine is not decrypted and the user sees an error message.

The script may return any value. To ensure best security, a value that includes only printable characters should be at least 32 bytes long. For binary data, the value should be at least 16 bytes long to ensure proper entropy. The output is sent to the StdOut file.

The following example is written in C. It is installed by Workstation as `sampleAuth.c`. Compile it with a C compiler if you want to run it.

```
#
# VMware Sample Script
#
# Sample script for ACE script authentication
#
# Description:
# This sample script looks up the user as defined in the environment
# variable TEST_USERNAME and returns seed data that is used to make a key
# for authentication purposes.
#
# It assumes that the username is defined in the environment variable
# TEST_USERNAME (a fictitious environment variable used for this sample)
# and returns the seed data from a hardcoded map of username to seed data.
#
# Input to script:
# None.
#
# Returns:
# 0 if successful (user is correctly authenticated).
# -1 if TEST_USERNAME is not set, or the user is unrecognized.
#
# Expected output:
# Seed data for creating script authentication key on stdout.
#
# Notes:
# If the script returns success, its output will be used to create a key.
# Therefore, it is important that the output of this script be unique for
# each user, and that there is enough data to make a meaningful key (at
# least 16 bytes).
```

```

#
#

my %user_map= ( 'charlie'      => 'E1C4F612135B4D98A33B2C9BD595025D',
                'kathy'       => 'C79AFFEF773D61225751C2566858DB08',
                'beth'        => '05B169B439B26AAB2EA4F755B7E3800C',
                'ernie'       => '8CE63D4AA2068BD8AFF2D1B05F3495A5',
                'bert'        => '"172B1619B2EFBE0E4F381AA1C428F049'
                );

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
    print "You should set the TEST_USERNAME environment variable.\n";
    exit(-1);
}

my $key_seed = $user_map{$username};
if (! defined $key_seed) {
    print "Unrecognized username.\n";
    exit(-1);
}

print $key_seed;
exit(0);

```

Example of a Host to Guest Data Script

The following example is written in Perl. It is installed by Workstation as `sampleQuarantine.pl`. You need a Perl interpreter to run this script.

```

#
#   VMware Sample Script
#
#   Sample script for ACE Host-Guest Data script
#
#   Description:
#   This sample script passes information defined on the host to the guest.
#   It assumes that the machine name is defined in the environment variable
#   TEST_MACHINENAME and that the asset tag is defined in the environment
#   variable TEST_ASSETTAG. (These are fictitious variables used for this #
#   sample).
#
#   Input to script:
#   None.
#
#   Returns:
#   0 if successful.
#
#   Expected output:

```

```

# Set of acceptable key/value pairs where the values are fetched from the
# environment variables. These values can be retrieved from within the
# Guest operating system using the VMware Tools.

my $machine_name = $ENV{TEST_MACHINENAME};
my $asset_tag = $ENV{TEST_ASSETTAG};
my $host_mac = $ENV{TEST_MACHINEMAC};

if (defined $machine_name) {
    print "machine.id = " . $machine_name . "\n";
}

if (defined $asset_tag) {
    print "guestinfo.assetTag = " . $asset_tag . "\n";
}

if (defined $host_mac) {
    printf "guestinfo.mac = " . $host_mac . "\n";
}

exit(0);

```

Example of a Power-On Hook Script

The following example is written in Perl. It is installed by Workstation as `sampleQuarantine.pl`. You need a Perl interpreter to run this script.

```

#
# VMware Sample Script
#
# Sample script for ACE power-on hook
#
# Description:
# This sample script implements a power-on hook for ACE. This can be used
# in addition to authentication to control the circumstances under which an
# ACE is allowed to run.
# This script assumes that the username is defined in the environment
# variable TEST_USERNAME (a fictitious environment variable used for this
# sample) and returns TRUE if the user is allowed to run, and FALSE
# otherwise.
# Input to script:
# None.
#
# Returns:
# TRUE if username is on white list.
# FALSE if username is not on white list or is undefined.
#
# Expected output:
# One of the strings "TRUE" or "FALSE"
#

```

```
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
    print "FALSE";
    exit(0);
}

my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
    print "TRUE";
    exit(0);
}

print "FALSE";
exit(0);
```

Customizing the VMware Player Interface on Windows Hosts Only

You can customize several aspects of the VMware Player user interface for ACE instances that run on Windows hosts. You save these customizations in a text file and identify that text file, called the skin file.

Create and Specify a Skin File

A skin file contains parameter settings for customizing the VMware Player user interface. Use this file to change application icons, the text that appears in the title bar, and to change the way removable devices are presented.

This feature is available only for VMware Player running on Windows hosts.

To create and specify a skin file

- 1 Use a text editor to create a skin file that includes the parameters to customize.

Use one line for each parameter and use the following form:

```
parameter = "value"
```

To comment out a line in the skin file, begin the line with the pound (#) sign.

- 2 Save the skin file in the ACE Resources directory in the virtual machine directory for the ACE-enabled virtual machine.

You can use any filename.

- 3 (Optional) To display application icons other than the VMware Player icon, place the new .ico icon files in the ACE Resources directory.

For icons sizes and skin file parameters, see [“Customizing the VMware Player Icons”](#) on page 408.

- 4 In Workstation, close the ACE-enabled virtual machine.
- 5 Use a text editor to open the aceMaster.dat file in the virtual machine directory and add the following line:

```
vmplayer.skin = "<filename>"
```

Because the skin file is in the ACE Resources directory, you do not need to specify the directory path to the file.

- 6 Save and close the aceMaster.dat file.

Customizing the VMware Player Icons

VMware Player has separate large and small application icons. The large icon is used in the application switching interface (visible when you press Alt+Tab). The size of the large icon is usually 32x32 pixels, but VMware Player uses whatever size is specified for icon size in the system preference. The small (16x16 pixels) icon is used in the VMware Player title bar and on the Windows taskbar button for VMware Player.

The icons used for these purposes must be in .ico file format and located in the ACE Resources subdirectory in the virtual machine directory. The applicable parameters in the skin file include the following:

```
player.iconSmall = "<filename>"
player.iconLarge = "<filename>"
```

One .ico file can contain multiple icons of different sizes. You can specify the same .ico file for player.iconSmall and player.iconLarge. VMware Player extracts the icon of the appropriate size for each use.

Customizing the Title Bar Text

You can specify what text appears in the VMware Player title bar. You can also specify the font and font size used to display the text.

The text displayed in the title bar consists of three sections: a prefix, the virtual machine name, and a suffix. The parameters listed in [Table 21-2](#) allow you to set any prefix and suffix, or to omit the prefix, the suffix, or both. They also allow you to include or omit the virtual machine name.

If you leave the defaults for all values, the title bar displays only the virtual machine name at 32 points in the MS Shell Dlg font.

[Table 21-2](#) describes the VMware Player title text parameters.

Table 21-2. VMware Player Title Text Parameters

Parameter	Type	Default	Controls
<code>player.title.prefix</code>	string	""	Title bar prefix
<code>player.title.useVMName</code>	Boolean	TRUE	Whether the virtual machine name is displayed
<code>player.title.suffix</code>	string	""	Title bar suffix
<code>player.title.font.face</code>	string	"MS Shell Dlg"	Font name (the font must be on the user's computer)
<code>player.title.font.size</code>	integer	32	Point size for the text

Customizing the Removable Device Display

Removable devices are represented in the VMware Player interface either by buttons on a toolbar or by menu items on a **Devices** menu. You can specify the type of display. You can also specify text, icon, or a combination of the two and specify custom icons.

If you use custom icons, copy the icon files to the ACE Resources directory in the virtual machine directory for the ACE-enabled virtual machine.

Settings you make in the skin file override any settings the user makes in the VMware Player preferences dialog box.

Use the following parameter to control whether devices are shown as toolbar items:

```
player.deviceBar.toplevel = [TRUE | FALSE]
```

Set the parameter to TRUE for a toolbar or FALSE for a menu.

Use the parameters shown in [Table 21-3](#) to customize the display for each removable device configured in the virtual machine.

Table 21-3. Removable Devices Parameters

Parameter	Type	Default	Controls
<code>player.deviceBar.<deviceName>.buttonStyle</code>	string (text, icon, texticon)	text	Appearance of toolbar button or menu item
<code>player.deviceBar.<deviceName>.buttonText</code>	string	User-friendly device name	Text that appears on the toolbar button or menu item when device is connected

Table 21-3. (Continued)Removable Devices Parameters

Parameter	Type	Default	Controls
player.deviceBar. <deviceName>.buttonTextD isconnected	string (optional)	Normal button text	Text that appears on the toolbar button or menu item when device is disconnected
player.deviceBar. <deviceName>.tooltip	string	""	Text that appears in the tooltip when device is connected
player.deviceBar. <deviceName>.tooltipDisc onnected	string (optional)	Normal tooltip	Text that appears in the tooltip when device is disconnected
player.deviceBar. <deviceName>.icon	filename	Icon representing this type of device	Custom icon file when device is connected
player.deviceBar. <deviceName>iconDisconne cted	filename (optional)	Normal icon	Custom icon file when device is disconnected
player.deviceBar. <deviceName>.shortcutKey	keySpec		Shortcut key combination to switch the device between connected and disconnected (see “Shortcut Key Values” on page 411)

Following are the device names you can use for <deviceName> in the parameter name:

- floppy0, floppy1
- serial0, serial1, serial2, serial3
- parallel0, parallel1, parallel2
- ide0:0, ide0:1, ide1:0, ide1:1 (IDE CD-ROM or hard drives)
- scsi0:0 – scsi0:7 (SCSI CD-ROM or hard drives)

Shortcut Key Values

Use virtual key codes to specify keyboard shortcuts. Virtual key codes use hexadecimal format, which is a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type **0x5A**.

Microsoft provides a reference list of virtual key codes on its MSDN Web site.

You can also use the Ctrl, Alt, and Shift modifier keys, or a combination of those keys. [Table 21-4](#) provides the shortcut key values.

Table 21-4. Shortcut Key Values

Modifier key	Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Ctrl+Alt	0x3
Alt+Shift	0x5
Ctrl+Shift	0x6
Ctrl+Alt+Shift	0x7

When you list a key plus a modifier, type the virtual key code for the key followed by a comma, followed by the value for the modifier key or keys. For example, the value entry for Ctrl+Shift+F1 is 0x70, 0x6.

Keep the following limitations in mind when defining shortcut keys:

- Do not use the Pause key with the Ctrl key.
- If you use F12, you must use one or more modifier keys. You cannot use F12 alone.

- You cannot use combinations that include only the Shift, Ctrl, and Alt keys. You can use these keys only as modifiers in combination with some other key.

Sample Skin File

```
player.title.prefix = "Our Company <<"
player.title.suffix = ">> Environment"
# player.title.useVMName = FALSE

# player.deviceBar.toplevel = TRUE
player.deviceBar.floppy0.buttonStyle = "icon"
player.deviceBar.floppy0.buttonText = "First Floppy Drive"
player.deviceBar.floppy0.shortcutKey = "0x30,0x7"
player.deviceBar.floppy0.icon = "custom-floppy.ico"
player.deviceBar.floppy0.tooltip = "Click to disconnect"
player.deviceBar.floppy0.tooltipDisconnected = "Click to connect"
# player.deviceBar.ethernet0.buttonStyle = "icon"
# player.deviceBar.idel:0.buttonStyle = "icon"
# player.deviceBar.audio.buttonStyle = "icon"
```

Deploying ACE Instances

22

This chapter provides instructions for specifying deployment settings for the packages, creating ACE packages, and deploying packages to end users. This chapter includes the following topics:

- [“Edit Deployment Settings”](#) on page 413
- [“Review the Configuration of an ACE-Enabled Virtual Machine”](#) on page 424
- [“Use Preview Mode to Test Policy and Deployment Settings”](#) on page 425
- [“Creating a Package”](#) on page 426
- [“Perform an End-to-End Deployment Test”](#) on page 431
- [“Deploy Packages”](#) on page 433

Edit Deployment Settings

Deployment settings enable you to configure package characteristics, such as instance customization and encryption, and then apply those settings to as many packages as you choose. Changes to deployment settings affect only packages created after the changes are made. They do not apply to existing packages.

Before you can use the deployment settings editor on a virtual machine, you must enable ACE features for that virtual machine. See [“Overview of Creating and Deploying ACE Packages”](#) on page 370.

To edit deployment settings

- 1 Select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.
- 2 In the deployment settings editor, select an item in the **Setting** list.

- 3 Complete the settings panel for that deployment setting and click **OK** or select another setting to edit.

For assistance with the fields on a settings panel, click **Help**.

Encryption Settings

Encryption settings are of two types:

- **Package encryption** – Protects package files from being copied or altered while in transit. If you set package protection to **Encrypted**, the New Package wizard encrypts the virtual machine when a package is created.
- **ACE instance encryption** – Protects ACE instance files from being copied or altered after installation and activation. You must specify an authentication method if you want the installer to encrypt the ACE instance.

The Workstation software uses defaults that the activation and authentication policies determine to apply encryption settings to the package and files. See [“Setting Access Control Policies”](#) on page 374.

The default encryption settings for deployment in production environments. The files do not need to be encrypted when you test deploy a package.

NOTE If you set the encryption settings to **None**, any verification specified in the resource signing policy is not performed. The encryption package setting overrides the resource signing policy setting. See [“Setting Resource Signing Policies”](#) on page 383.

Package Lifetime Settings

You can specify a time period during which an ACE package is installable. If a user attempts to install a package outside of this time period, an error message appears and the package is not installed.

The administrator can change the package lifetime settings on managed packages even after package creation.

Change Package Lifetime Settings for a Managed Package

If you use the ACE Management Server, you can change the package lifetime settings or deactivate a package immediately.

Make sure Workstation is connected to the ACE Management Server. For information about installing and setting up the server, see the *ACE Management Server User's Guide*.

To change package lifetime settings for a managed package

- 1 Select the ACE-enabled virtual machine and choose **View > Current View > Summary**.
- 2 Right-click the package you want to change in the **Package History** section at the bottom of the summary tab.
- 3 Do one of the following:
 - To change the package lifetime settings choose **Properties > Settings**.
 - To deactivate the package immediately choose **Deactivate**.

Instance Customization on Windows Hosts Only

Instance customization applies only to ACE instances that have a Windows guest operating system installed. The instance customization process is built around the standard Microsoft Sysprep deployment tools. It provides the following benefits:

- Automates the Sysprep process (the use of the Microsoft Sysprep deployment tools). It gives you better control of some Sysprep parameters, such as computer name.
- Automates joining ACE instances to a domain from a remote site. See [“Set Up a Remote Domain Join”](#) on page 420.
- For managed ACE instances, the instance customization process on the user’s machine reports the success or failure of the process to the server. The information is available in the instance view of Workstation. Besides status, the process also reports the MAC address and the new computer name.

Instance Customization Process During Packaging

If you specify instance customization deployment settings, the following events occur when you complete the New Package wizard:

- 1 A snapshot of the ACE-enabled virtual machine is taken and saved.
- 2 The ACE-enabled virtual machine is powered on, and all the required deployment tools and files, including the appropriate Microsoft Sysprep tools, are copied into the guest.

No visible indication shows the copying process. See [“Download the Microsoft Sysprep Deployment Tools”](#) on page 417.

- 3 The Microsoft deployment tools run inside the guest operating system to seal the guest and prepare for deployment.

- 4 The guest operating system shuts down.
- 5 The ACE-enabled virtual machine is cloned into the package directory.
The virtual machine files are copied into the directory, encrypted if set to do so, and divided to be put on media if set to do so.
- 6 The ACE-enabled virtual machine reverts to the snapshot.
- 7 The snapshot is deleted.
- 8 The installer files are copied into the package directory.

Instance Customization on the End User's Machine

On the ACE user's machine, after the installation and instance activation, the following events occur:

- 1 All information required for resolving placeholder variables is obtained.
- 2 Placeholder variables are resolved and replaced with the actual values for the ACE instance.

See [“Placeholder Values to Use in Instance Customization”](#) on page 419.
- 3 The Microsoft Mini-Setup process runs unattended.
If the Mini-Setup process fails, the ACE instance shuts down.
- 4 (Optional) Additional commands to execute other scripts that you specified in the instance customization deployment settings are executed.
- 5 (Optional) If you configured a remote domain join, the software executes the script you specified, connects the ACE instance to the VPN server, and joins the virtual machine to the domain.

See [“Set Up a Remote Domain Join”](#) on page 420.)
- 6 For managed instances, instance customization is reported to the server if it is successful.

Prerequisites for Using Instance Customization

Instance customization is available for both managed and standalone ACE instances.

Before you specify instance customization settings, perform the following tasks:

- Install a Windows 2000, XP Professional, Server 2003, or Vista guest operating systems on your ACE-enabled virtual machine.

- Install the latest version of VMware Tools on the guest operating system. See [“Installing VMware Tools”](#) on page 105.
- Download the Microsoft Sysprep tools. See [“Download the Microsoft Sysprep Deployment Tools”](#) on page 417.
- Gather the following information:
 - The Windows product ID for the guest operating system installation.
 - If the ACE instance will be joined to a domain (whether the instance is local or remote to the domain), the user name and password for an account that has permission to add computers to the domain.
 - Remote domain join parameters if a remote ACE instance will be joined to a domain. See [“Set Up a Remote Domain Join”](#) on page 420.

Download the Microsoft Sysprep Deployment Tools

You do not need to download Microsoft Sysprep deployment tools if you have a Windows Vista operating system. They are included with the Windows Vista installation.

To download the Microsoft Sysprep deployment tools

- 1 Go to the Microsoft Web site and search for Sysprep deployment tools.
- 2 Follow the instructions on the site for downloading the Sysprep deployment tools.

Download all versions that correspond to the guest operating systems that you plan to deploy. These tools include Sysprep deployment tools for Windows 2000, Windows 2003, and Windows XP Professional SP1 and SP2. The SP1 version works with Windows XP Professional with no service pack and Windows XP Professional SP1.

- 3 Unzip the files into the directory where Workstation is installed.

The default installation directory is:

```
C:\Program Files\VMware\VMware Workstation
```

Specify Deployment Settings for Instance Customization

Before you begin, install all required files for customization scripts. See [“Prerequisites for Using Instance Customization”](#) on page 416.

To specify deployment settings for instance customization

- 1 Select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.
- 2 Select **Instance Customization** and complete the settings panel.
- 3 Select **System Options** and complete the settings panel.

Use the following information to complete the fields:

- **System options** – You can use placeholder variables for the system name, organization name, and computer name. For details on the placeholder variables, including an example, see [“Placeholder Values to Use in Instance Customization”](#) on page 419.



CAUTION The Mini-Setup process fails if you enter **administrator** in the **Name** field or the **Computer Name** field or for Windows Vista guests, if the computer name is more than 15 characters.

If you set the %logon_user% placeholder in those fields and the placeholder variable resolves to **administrator**, the software automatically changes the value to a random alphanumeric string of 10 characters.

- **Security ID** – A new SID is always generated for Windows Vista guests, regardless of the setting you choose here.
- 4 Select **Initialization Scripts** and type the additional commands to run scripts in the guest operating system at the end of the Mini-Setup process on the ACE user's machine.

For more information about commands, see the Microsoft deployment tools documentation.

NOTE Specify the path to the batch file without using quotation marks. Quotation marks are added automatically.

For more information, see the Microsoft knowledge base article about troubleshooting `Cmdlines.text` during an unattended setup.

- 5 Select **Workgroup or Domain** and complete the settings panel using the following information:
 - Instance customization supports only IP addresses that DHCP servers provide. Static IP addresses are not supported.

- To allow this ACE instance to join the domain from a location remote to the domain, see [“Set Up a Remote Domain Join”](#) on page 420.

6 Specify other types of deployment settings or click **OK**.

To create a package with these settings, see [“Creating a Package”](#) on page 426.

Placeholder Values to Use in Instance Customization

Use placeholder values to construct machine-specific names inside the guest operating system during the Mini-Setup process.

Following are the available placeholders:

- `%logon_user%` or `%logon_user(n)%` – The user logged in to the host machine at the time the Microsoft Mini-Setup process begins.

You can use `%logon_user(n)%`, where `<n>` is the maximum number of characters obtained from the actual logged-in user when the name is resolved. Use `<n>` if the user name must be resolved to no more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual user name and you want to limit the resolved name to 15 characters, set `<n>` to 12. Your entry in the **Name** field in the **System Options** panel is `%logon_user(12)%random_alpha_digit(3)%`.

Including `(n)` in the placeholder is optional. If you use only `%logon_user%` or if you set `<n>` to zero (0), the placeholder resolves to the full logged-in user name.

- `%host_name%` or `%host_name(n)%` – The name of the host computer (usually used with some additional random number or name).

You can use `%host_name(n)%`, where `<n>` is the maximum number of characters obtained from the actual computer host name when the name is resolved. Use `<n>` if the host name must be resolved to not more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual host name and you want to limit the resolved name to 15 characters, set `<n>` to 12. Your entry in the **Computer Name** field in the **System Options** panel is `%host_name(12)%random_alpha_digit(3)%`.

Including `(n)` in the placeholder is optional. If you use only `%host_name%`, or if you set `<n>` to zero (that is, the placeholder resolves to the full host name.

- `%random_alpha_digit(n)%` – A randomly generated string of alphabetic and numeric characters, where `<n>` is the number of characters. You must specify `<n>`.
- `%random_alpha(n)%` – A randomly generated string of alphabetical characters, where `<n>` is the number of characters. You must specify `<n>`.

- `%random_digit(n)%` – A randomly generated string of numeric characters, where `<n>` is the number of characters. You must specify `<n>`.

For Windows Vista guests, if the computer name is more than 15 characters, the Mini-Setup process fails on the user machine.

Specify Additional License Information for Windows Server Products

To supply additional license information for Windows Server products, you can add a file named `sysprep_license.txt` to the ACE-enabled virtual machine directory.

To specify additional license information for Windows Server products

- 1 Use a text editor to create a skin file named `sysprep_license.txt` in the virtual machine directory for the ACE-enabled virtual machine.

- 2 Add the following line to the file:

`AutoMode=[PerSeat | PerServer]`

This line indicates whether the license is for one client license or for a certain number of client licenses for a server.

- 3 If `AutoMode` is set to `PerServer`, add the following line to the file, `<n>` indicates the number of client licenses for the server:

`AutoUsers=<n>`

- 4 Save and close the file.

For more information, go to the Microsoft TechNet Web site and in the Windows Server Library, search for [LicenseFilePrintData] (Sysprep).

If this file is not found in the virtual machine directory, a default is used. `AutoMode` is set to `PerServer` with 5 client licenses.

If you supply this file, the license portion of the Mini-Setup process appears unchanged during preview. You always see `AutoMode=PerServer` and `AutoUsers=5` in the Mini-Setup user interface. The license information you supply is nevertheless set correctly by the Mini-Setup process.

Set Up a Remote Domain Join

The remote domain join feature provides an automated way to join ACE instances to a domain from a remote site.

After the ACE package is installed on the end user's machine and the ACE instance is activated and authenticated, the Microsoft Mini-Setup process runs. The script for

joining the remote ACE instance to the domain executes at the end of that process, and the machine is joined to the domain.

Before you begin, perform the following tasks:

- Determine which VPN client to download. The VPN client must support a command-line interface so that a script can be used for logging in to the VPN server. You might need to contact the VPN product's technical support to find out whether the VPN client supports a command-line interface.
- Obtain a VPN account for logging in to the server. Credentials include a user name and password. Randomly generated security tokens cannot be used as passwords. For example, you cannot use an RSA security token.
- Determine the following information to use for the VPN client profile: the company's group and password information and the name of the VPN server to contact to establish a secure connection.
- Determine the name of the domain that you plan to add the ACE instance to.
- Determine the user name and password for an account that has permission to add computers to the domain.

To set up a remote domain join

- 1 In the guest operating system of the ACE-enabled virtual machine, install a VPN client that supports a command-line interface.
- 2 Use the VPN client software to configure a profile for this client.

The profile in the VPN client contains a company's group and password information and determines which server to contact to establish a secure connection.
- 3 Write a .bat script that allows remote execution during the instance customization process.

Following is an example of a .bat script for a Cisco VPN client:

```
"net" start "Cisco Systems, Inc. VPN Service"
"C:\Program Files\Cisco Systems\VPN Client\vpnclient.exe" connect
    <profile_name> user <vpn_user_name> pwd %1 >> vpnlogs.txt
```

This example consists of two lines. The command in the first line starts the Cisco VPN client's background service. The command in the second line connects to the Cisco VPN using a command-line interface. It supplies the name of the VPN profile and the credentials for logging in to the VPN server. The example uses the password placeholder variable, but you could also use a static password for the VPN account. A static password included in a script is sent in clear text.

- 4 Save the **.bat** file on the **C:** drive of the guest's file system.
- 5 In Workstation, select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.
- 6 Select **Workgroup or Domain**.
- 7 In the settings panel, select **Domain** and specify a user name for an account that has permission to add computers to the domain.

If the ACE-enabled virtual machine is managed, passwords and commands are stored on the ACE Management Server.

If the ACE-enabled virtual machine is standalone, passwords and commands are stored with the package. Be sure to use encryption for the package.

- 8 Select **Enable Remote Domain Join**.
- 9 Specify the password for logging in to the VPN server.
You can then use the **%password%** placeholder variable in the **Command** text box to refer to this password.
- 10 Enter the command that executes the script.

For example, if you name the **.bat** script **vpn.bat** and want to use the password placeholder variable, enter the following command:

C:\vpn.bat%password%

If you use a password placeholder variable (**%password%**) in the **Command** field, the placeholder variable is resolved and replaced with the value from the **Password** field when the script executes.

- 11 Click **OK** to save the settings.

To create a package with these settings, see [“Creating a Package”](#) on page 426.

Custom EULA Settings

You can provide a custom End-user license agreement (EULA) that appears when an ACE instance is activated. The user must see and accept before the instance can run for the first time.

The custom EULA must be a text file located in the **ACE Resources** directory for the ACE-enabled virtual machine. The file can use the following formats:

- For Windows hosts, use a **.txt** or **.rtf** file.
- For Linux hosts, use a **.txt** file.

- If you plan to deploy the package to both Windows and Linux computers, use a `.txt` file.

To specify whether to deploy to Windows hosts, Linux hosts, or both, use the **Deployment Platform** setting in the deployment settings editor.

Deployment Platform Settings

By default, ACE packages are created for Windows hosts. Change this setting to deploy to Linux or both Linux and Windows hosts.

ACE Resources Directory

The ACE Resources directory is a subdirectory of the ACE-enabled virtual machine's directory. All files placed in this directory are copied into the ACE package so that they can be used in end users' virtual machines.

Place the following types of files in the ACE Resources directory:

- Authentication scripts
See [“Create and Deploy an Authentication Script”](#) on page 377.
- Power-on and power-off scripts
See [“Include a Power-On and Power-Off Script in the Package”](#) on page 378.
- Other resource files that authentication, power-on, or power-off scripts call
- Device files such as ISO images or FLP images that the virtual machine is configured to point to
- The skin file, which you can create to customize the VMware Player icons, removable device icons, and title bar text used in the VMware Player user interface on Windows guests
See [“Create and Specify a Skin File”](#) on page 407.
- Icon files for removable devices or the VMware Player application
See [“Customizing the VMware Player Icons”](#) on page 408 and [“Customizing the Removable Device Display”](#) on page 409.
- Custom EULAs
See [“Custom EULA Settings”](#) on page 422.

When you use the ACE Resources directory, take the following considerations into account:

- Do not place files in a subdirectory of the ACE Resources directory. If scripts or skin files reference other files, place those other files in the main ACE Resources directory. Make sure the script uses relative paths to reference those resources.

A resource is considered any file in the ACE Resources directory. You can specify whether to verify all files in the ACE Resources directory or just the policy scripts in that directory. For more information, see [“Setting Resource Signing Policies”](#) on page 383.

- If you change a policy or package setting that requires the ACE Resources directory, you must create an update package to deploy the change to end users.

Review the Configuration of an ACE-Enabled Virtual Machine

To finish preparing your ACE-enabled virtual machine and its files for packaging, review its configuration and policies and ensure that the appropriate operating system and software are installed in it.

To review the configuration of an ACE-enabled virtual machine

- 1 Verify that the ACE-enabled virtual machine has the necessary operating system, application software, and VMware Tools installed.

See [“Installing VMware Tools”](#) on page 105. For information about specific operating systems, see the *VMware Guest Operating System Installation Guide*.

- 2 To review configuration settings, select the ACE-enabled virtual machine and choose **View > Current View > Summary**.
- 3 To review virtual machine devices and virtual hardware, click the **Devices** tab in the summary view.
- 4 To review virtual machine configuration options, click the **Options** tab.
- 5 To make changes to devices or options, click **Edit virtual machine settings** in the **Commands** list.
- 6 To review policies and deployment settings, click the **ACE** tab.
- 7 To make changes to policies or deployment settings, click **Edit policies** or **Edit deployment settings** in the **Commands** list.

Use Preview Mode to Test Policy and Deployment Settings

Preview mode enables you to run an ACE instance as it runs on an end user's machine. You can see the effects of changed policies without having to package and deploy them. Preview mode also enables you to see the effects of setup choices without having to create, deploy, and install a full package.

You can run the ACE instance in preview mode in VMware Player and also run the ACE-enabled virtual machine in Workstation without having to shut down the preview.

NOTE You can run any ACE-enabled virtual machine directly in Workstation to be sure that the guest operating system and applications perform as expected. However, an ACE-enabled virtual machine running in Workstation does not respect any policies that restrict its functionality.

Before you begin, verify that the settings and deployment platforms you want to test are appropriate for preview mode. Because Workstation runs only on Windows hosts, you cannot use preview mode to run ACE instances as they run on Linux hosts. You also cannot test a host policy in preview mode. To test ACE instances that you plan to deploy on Linux hosts, or for which you want to test a host policy, see [“Perform an End-to-End Deployment Test”](#) on page 431.

To use preview mode to test policy and deployment settings

- 1 Open the ACE-enabled virtual machine to test.
- 2 In the summary view, click **Edit policies** in the **Commands** list.
- 3 In the **Policy** list, select the policy to change, complete the settings panel for that policy, and click **OK**.
- 4 In the summary view, click the **Preview in Player** in the **Commands** list.

A package based on a linked clone is created in a new directory, **Preview Deployment**, inside the ACE-enabled virtual machine's directory. The linked clone is created from a snapshot of the virtual machine's current state. Unlike a package that is deployed to an ACE user's machine, this package is not installed.

VMware Player allows you to activate and authenticate the ACE instance (if those policies are set). If configured, instance customization is also performed. The guest operating system starts.

- 5 Test the policy change in the running ACE instance to ensure that it is the one you want to make.

Preview mode enables VMware Player to run interactively so that you can see any instance customization errors and make corrections as needed.

- 6 (Optional) To make additional changes to policies or deployment settings, shut down the virtual machine and repeat this procedure.

You can have only one preview instance per ACE-enabled virtual machine. When you click **Preview in Player** a second or subsequent time, a message asks if you want to replace the current preview instance with a new deployment or use the existing deployment.

To change only policies and not repeat the activation and instance customization steps, use the existing deployment.

- 7 If an ACE Management Server is managing the virtual machine, click **Publish Policies to Server**.

Creating a Package

After you create an ACE-enabled virtual machine and configure policies, devices, and deployment settings, use the New Package wizard to create a package to deploy instances to users.

NOTE To create a Pocket ACE package for distribution on portable devices, use the Pocket ACE Package wizard rather than the New Package wizard. See [“Create a Pocket ACE Package”](#) on page 436.

For packages that you plan to deploy to Windows hosts, you can specify that the package is to be distributed through a network image or through DVDs or CDs. For DVD and CD distribution, the package is divided into files that fit on standard discs.

Overview of Package Creation and Validation

Depending on whether you want to deploy a new ACE instance or update an installed one, you can create any of the following types of packages:

- **Full package** – Includes an installer and the additional files needed to install an ACE package and the VMware Player application that runs the ACE instance. A full package allows you to create a completely new ACE instance.



CAUTION If you replace an existing ACE instance by supplying a new full package, end users lose any data or custom settings stored in it.

- **Policy update package or Server update package** – Includes just the policy-related files.
 - For standalone ACE-enabled virtual machines, the option is **Policy Update**.
 - For managed virtual machines, it is **Server Update**.

Among other policies, a server update package allows you to change the server that the ACE-enabled virtual machine is associated with or change an activation-only server setup to an activation and tracking setup.
- **Custom package** – Allows you to choose specific items to deploy.
- **Pocket ACE package** – The components for a Pocket ACE package vary slightly from those for the full package. For information about the Pocket ACE package, see [“Create a Pocket ACE Package”](#) on page 436.

The deployment settings and device settings that you already set for an ACE-enabled virtual machine allow you to create multiple packages quickly. You can use the same settings again and again.

Package validation occurs after you complete the New Package wizard. Package validation does the following:

- Checks that all files that the ACE-enabled virtual machine requires are present. Those files include:
 - Disk and snapshot files
 - Script files (if any policy is using scripts)

NOTE Package validation does not check for device files (ISO images, FLP images, and so on). To include device files in the package, put the files in the ACE Resources folder for the ACE-enabled virtual machine and set the devices to point to that location.

- Checks that the ACE-enabled virtual machine can be cloned: that it is powered off, multiple snapshots are enabled, and it is not read-only.
- Checks that the latest version of VMware Tools is installed.
- If instance customization is enabled, checks that the SysprepTools directory for the ACE-enabled virtual machine’s guest operating system is not empty.
- If the guest operating system is Windows 2000, Windows XP, or Windows 2003, checks that the folders in the Program Files\VMware\VMware Workstation\Resources\SysprepTools folder are not empty.

You can deploy a package over a network or on DVD or CD. If you deploy the package on discs, the first disc of the set includes the autorun files needed to start the installer automatically when the user inserts the disc in the host computer's drive.

Turn Off the VMware Tools Check for Test Deployments

If you do not have the latest version of VMware Tools installed in the guest operating system, the wizard fails to create the package. To create packages without installing the latest Tools version each time—for example, if you want to perform a test deployment of these packages and don't need the latest Tools in the resulting instances to run your tests—you can turn off the Tools check.

To turn off the VMware Tools check for test deployments

- 1 Close Workstation.

Use a text editor to open the `preferences.ini` file, which is located in the `C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation` directory.

- 2 Add the following line to the file:

```
pref.ignoreToolsPkgCheck = "TRUE"
```

Setting this line to FALSE reinstates the VMware Tools check.

- 3 Save and close the `preferences.ini` file.

Before you create packages that you plan to deploy in production environments, reinstate the VMware Tools check.

Prerequisites for Using the Packaging Wizards

The following prerequisites apply to the New Package wizard and the Pocket ACE Package wizard:

- Ensure that the guest operating system and the most recent version of VMware Tools are installed in the ACE-enabled virtual machine. See [“Installing VMware Tools”](#) on page 105.
- Defragment virtual disks to ensure that the package is as compact as possible. See [“Defragment Virtual Disks”](#) on page 217.
- Preview the ACE instance to verify that all settings are working correctly. See [“Use Preview Mode to Test Policy and Deployment Settings”](#) on page 425.
- Determine the passwords used for the policies and deployment settings. These can include the following:

- **Activation password** – Access control policy is set to **Password**.
- **Domain join credentials** – Access control policy for the ACE instance is set to **Password**, and the **Instance Customization** deployment setting for **Domain** is enabled. This password is for the user account that has permission to add computers to this domain.
- **Remote domain join credentials and VPN credentials** – The **Instance Customization** deployment settings for **Domain** and **Enable remote domain join** are enabled. The domain password is for the user account that has permission to add computers to this domain. The password in the **Remote domain join** section is for the user account that has permission to access the VPN server.
- Verify that you have enough disk space for temporary files created during packaging. You must have twice the combined sizes of all the components of the package.

The wizard displays information about the amount of space needed and the locations where the space is needed. If you do not have enough free space, a warning message appears. You can move or delete files on the target drives to make room for the wizard's working files.
- Determine the type of package you want to deploy: full, update, or custom. See [“Overview of Package Creation and Validation”](#) on page 426.
- To distribute the package on DVDs or CDs, determine how much disk space is available. You can then specify the maximum file size used when the package is divided into multiple files.

To use instance customization, verify that the following prerequisites are satisfied:

- Make sure that the guest operating system is Windows XP, Windows 2000, or Windows 2003.
- Copy the Microsoft Sysprep Deployment Tools into the correct folder for the virtual machine. See [“Download the Microsoft Sysprep Deployment Tools”](#) on page 417.

If these tools are not available, the packaging operation fails. The failure might not occur until well into the packaging process and might cause you to lose substantial time.

- Use preview mode to test whether instance customization runs unattended. For example, verify that a valid Windows product ID is used so that no dialog box prompts for the product ID during the Mini-Setup process.

- If you configured automatic login, use preview mode to verify that automatic login works correctly. If it fails, instance customization fails.

Use the New Package Wizard

The New Package wizard creates an executable file that contains an ACE-enabled virtual machine, its policies, deployment settings, scripts, and a copy of VMware Player. You can easily deploy and install the package on end user's machines.

Before you begin, verify that the packaging prerequisites are satisfied. See [“Prerequisites for Using the Packaging Wizards”](#) on page 428.

To use the New Package wizard

- 1 Open the ACE-enabled virtual machine to use as the basis for the package.
- 2 Make sure the virtual machine is powered off rather than suspended.

When you exit preview mode, by default VMware Player suspends the virtual machine. If necessary, use Workstation to power off the virtual machine.

- 3 Choose **VM > ACE > New Package**.
- 4 Complete the New Package wizard.
- 5 (Optional) If you are prompted to select a package distribution format and you select **Multiple folders for creating DVDs or CDs**, write down the disc label prefix you specify.

When you later use disc-burning software to create the discs, the name you enter for each disc must be the same as the name of the folder the wizard creates to hold that disc's contents (for example, DISC1, DISC2).

- 6 To begin the packaging process, click **Next** on the Package Summary page.

Package creation takes a substantial amount of time, especially for packages that include large virtual machines or instance customization settings.

During the instance customization stage, if the guest operating system does not shut down after approximately 10 minutes, the problem might be that the Sysprep tools were not in place. The operation is cancelled and an error message tells you that instance customization failed.

The Package Creation Complete page appears when the process is complete. It lists the location of the newly created package and provides a link to the package directory.

- 7 Depending on which distribution method you chose, do one of the following:

- If you created a single file for network distribution, copy the file to the appropriate location on a network.
- If you created one or more files for distribution on CD or DVD, use disc-burning software to create the discs.

The disc label you enter in your disc-burning software for each disc must be the same as the name of the folder the wizard creates to hold that disc's contents.

- Burn the contents of each disc onto the top level of the disc.

The package installer expects to find only the contents of the folder, and not the folder itself, at the root level on the disc. If you burn the folder itself onto the disc, when you attempt to install the contents of the second or subsequent discs on the user's machine, the error 1309, "Error reading from file <filename>", appears.

View Package Properties and Add Notes

Use the Package Properties dialog box to view properties of the packages that you created. Also add or edit notes that appear in the summary view of the ACE-enabled virtual machine.

To view package properties and add notes

- 1 Open the ACE-enabled virtual machine.
- 2 Choose **View > Current View > Summary**.
- 3 In the **Package History** section of the view, double-click the package.
You might need to scroll down to find the **Package History** section.
- 4 Click the tabs to view the properties.
- 5 Click the **Notes** tab to add or edit notes.

Existing notes might have been added when the package was created using the New Package wizard. These notes are not be seen by end users. They are visible only in the Workstation window.

Perform an End-to-End Deployment Test

Perform an end-to-end test to deploy a new ACE package rather than a package update. Also use an end-to-end test if using preview mode is not appropriate.

Because Workstation runs only on Windows hosts, you cannot use preview mode to run ACE instances as they will run on Linux hosts. You also cannot test a host policy in preview mode.

NOTE This test might take a long time because packaging and encryption processes can be lengthy.

Before you begin, if you plan to use an ACE Management Server to manage the ACE instances, install and configure a test ACE Management Server. See the *VMware ACE Management Server User's Guide*.

To perform an end-to-end deployment test

- 1 If you use the ACE Management Server, select the ACE-enabled virtual machine, choose **File > Connect to ACE Management Server**, and connect to the test server.
- 2 In the virtual machine's summary view, click **Create new package** in the **Commands** list.
- 3 Complete the New Package wizard.
- 4 Navigate to the package location and copy the package directory to a client test machine.
- 5 On the client test machine, run the ACE instance's `setup.exe` file and complete the pages of the installation wizard.

Depending on how you configured the package, a **Start** menu item or a desktop shortcut or both are created on the client machine. Depending on the runtime preferences you set, the ACE instance might start in full screen mode when the host system starts.

- 6 Start the ACE instance and activate it when prompted.
- 7 Verify that the ACE instance is configured as you intended and runs as you expect.
- 8 If you use the ACE Management Server, connect the ACE-enabled virtual machine to the production server.

On the administrator machine, in Workstation, select the ACE-enabled virtual machine and choose **File > Connect to ACE Management Server**, and connect to the production server.

- 9 If you use the ACE Management Server, create a new package.

The package you created for the test refers to the server you used for testing. Instances created from that package refer to the test server.

Deploy Packages

Deploying packages means making the ACE package available to end users. You specify the distribution method when you create the package.

To deploy packages

Depending on the type of package, do one of the following:

- For a full, policy update, server update, or custom package, distribute the package on CD or DVD, or make the package available on a network.
- For a Pocket ACE package, see [“Deploying the ACE Package on a Portable Device”](#) on page 437.

Beta

Beta

The Pocket ACE feature enables you to store ACE instances on portable devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, and portable hard drives. ACE users attach these portable devices to x86 host computers, run their ACE instances with VMware Player, and then detach the portable devices. The next time they need access to their ACE instances, they can attach the devices to the same host computers or to different computers.

Use Pocket ACE to package a daily computing environment and allow end users to take that environment—including documents, settings, applications, and VPN access—wherever they need to go.

This chapter includes the following topics:

- [“Portable Device Requirements”](#) on page 435
- [“Policies and Deployment Settings for Pocket ACE”](#) on page 436
- [“Create a Pocket ACE Package”](#) on page 436
- [“Deploying the ACE Package on a Portable Device”](#) on page 437
- [“Run the Pocket ACE Instance”](#) on page 439

Portable Device Requirements

You can install ACE packages on the following types of devices:

- Flash memory drives (USB keys)
- Flash-based Apple iPod mobile digital devices
- Hard drive-based Apple iPod mobile digital devices
- Portable hard drives

For USB devices, use USB 2 high-speed devices only.

When a Pocket ACE package is deployed to a removable device, the virtual disk is preallocated to full capacity for enhanced performance. Make sure that the removable device has enough disk space to store the virtual disk's total capacity, memory, and approximately 300MB for overhead. See [“Using the New Virtual Machine Wizard”](#) on page 92.

Policies and Deployment Settings for Pocket ACE

Some policies apply only to Pocket ACE. You can set Pocket ACE close behavior by editing the runtime preferences policy.

Close behavior determines whether the ACE instance is powered off or suspended when the user exits and whether changes are synchronized on the removable device. See [“Pocket ACE Cache Settings”](#) on page 397.

Pocket ACE ignores some policies. Although you can set host and snapshot policies and create a package that includes them, Pocket ACE instances ignore these policies. Administrators cannot revert to reimage snapshots when running a Pocket ACE in administrator mode in VMware Player.

Create a Pocket ACE Package

Before you begin, determine the following information, which is specific to Pocket ACE:

- Does the portable device meet the hardware and disk space requirements for Pocket ACE. See [“Portable Device Requirements”](#) on page 435.
- Do you want to deploy the Pocket ACE to Windows machines, 32-bit Linux machines, 64-bit Linux machines, or some combination. Your choices affect the disk space requirements.
- What is the password you want to use for anyone who attempts to deploy the package to a portable device.

If you do not want to require a password, make sure the access control policy's authentication type is set to **None**. Make sure the encryption deployment setting for package protection is set to **None**.

In addition, complete the tasks listed in [“Prerequisites for Using the Packaging Wizards”](#) on page 428.

To create a Pocket ACE package

- 1 Open the ACE-enabled virtual machine to use as the basis for the package.
- 2 Make sure the virtual machine is powered off rather than suspended.

When you exit preview mode, by default VMware Player suspends the virtual machine. If necessary, use Workstation to power off the virtual machine.
- 3 Choose one of the following:
 - To create a new Pocket ACE, choose **VM > ACE > New Pocket ACE Package**.
 - To create an update package for a Pocket ACE, choose **VM > ACE > New Package**.
- 4 Complete the wizard.

When you specify a location on the Name the Package page, choose a location on the administrator machine. Do not specify a location on the portable device. You deploy the package to the device after the package is created.

The Completing the Pocket ACE Package Wizard page appears when the process is complete.

- 5 (Optional) To deploy the package immediately, select **Deploy to a portable device now**.

If you do not deploy the package immediately, see [“Deploying the ACE Package on a Portable Device.”](#)

Deploying the ACE Package on a Portable Device

You can deploy multiple ACE packages on a single portable device. The only limitation on the number of packages is the amount of available space on the device. You run the `deploy.exe` file to deploy individual ACE instances or the `bulkDeploy.exe` file to deploy ACE instances to multiple devices.

The wizard automatically preallocates disk space and splits the disk into 2GB segments.

The Pocket ACE instance is reencrypted during the deployment instead of after the user’s first run of the instance. For this reencryption, the policy applied is the package protection policy that was in place at the time of packaging.

Deploy a Single Pocket ACE Package to a Device

Before you begin, make sure the removable device meets the hardware and disk space requirements. See [“Portable Device Requirements”](#) on page 435.

To deploy a single Pocket ACE package to a device

- 1 Navigate to the package location you specified in the New Pocket ACE Package wizard.
- 2 Run the `deploy.exe` file.
- 3 If the Enter Password dialog box appears, enter the deployment password.
- 4 Complete the VMware Pocket ACE Deploy Utility dialog box.

When you distribute the Pocket ACE, give it directly to the user and tell the user to keep the Pocket ACE secure until the user runs the ACE and changes the user password.

Deploy Multiple Pocket ACE Packages to a Device

Before you begin, make sure the removable device meets the hardware and disk space requirements. See [“Portable Device Requirements”](#) on page 435.

To deploy multiple Pocket ACE packages to a device

- 1 Open a command prompt and change directories to your bulk deployment directory.

For example, enter the following command:

```
cd C:\Documents and Settings\Administrator\My Documents\  
Virtual Machines\ACE-Enabled Virtual Machine\Packages\Pocket ACE Package
```

- 2 Enter the following bulk deployment command and specify the necessary parameters:

```
bulkDeploy.exe <drive> <parameters>
```

Parameter	Usage
-p	Deployment password. Required when the package is password protected.
-s	Path to the VMX file on the host system. Use this parameter if you are performing a bulk deployment from outside of the Pocket ACE package.
-q	Parameter to turn off reporting the progress of the bulk deployment.
-t	Tests the bulk deployment without actually performing it. If the test fails, the bulk deployment fails. If the test is successful, 0 is returned. If it fails, a negative number is returned.

For example,

```
bulkDeploy.exe C: -p password -s C:\pocketACEPackage\VM\packagedVMX.vmx
-q -t
```

Run the Pocket ACE Instance

After you deploy a Pocket ACE package to a removable device, running it usually involves only plugging it in.

Before you begin, make sure that the host computer's clock is set to the correct time. If you move a Pocket ACE from one host computer to another and the clock of the second host is earlier than the clock of the first, the Pocket ACE does not run.

When the ACE instance runs, its disk and checkpoint caches are initialized. If the Pocket ACE has a session on this host, that session continues. Otherwise a new session is started.

The checkpoint state and virtual disk are cached on the host during use and synchronized back to the portable device later. The checkpoint state and virtual disk are protected with the same encryption level used for the ACE instance on the portable device.

The Pocket ACE runs primarily from the host cache, although it occasionally reads from the parent disk on the portable device. The ACE instance does not write to the parent disk.

To run a pocket ACE instance

- 1 Plug the portable device into the host computer.
- 2 If the host system's autorun configuration is not set to start the ACE instance automatically, do one of the following:

- On Windows hosts, navigate to the removable device and run the Pocket ACE.

Usually, starting the Pocket ACE manually is not necessary. The autorun program is included in the package and checks whether VMware Player is installed. If not, VMware Player is installed automatically.

- On Linux systems, install VMware Player from the `Player` directory on the USB drive.

For example, if the USB drive is mounted at `/media/USBFLASH`, navigate to `/media/USBFLASH/player/VMware-player.i386.tar.gz`.

- Install VMware Player as described in [“Manually Install VMware Player on a Linux Host”](#) on page 445.

- Use VMware Player to open the .vmx file and start the ACE instance (see [“Install the ACE Instance on a Single Linux Host”](#) on page 446).

Beta

Installing ACE Instances

This chapter includes the following topics:

- [“Installing an ACE Package on a Windows Host”](#) on page 441
- [“Installing an ACE Package on a Linux Host”](#) on page 444
- [“Start and Use an ACE Instance”](#) on page 447
- [“Install an ACE Client License”](#) on page 448
- [“Quit VMware Player”](#) on page 449
- [“Troubleshooting Tools”](#) on page 450

Installing an ACE Package on a Windows Host

If an end user’s computer does not already have VMware ACE or VMware Player installed, the first time you install an ACE package, VMware Player is installed along with the ACE instance.

You can install ACE instances on one host at a time, or you can use the silent installation features of the Microsoft Windows Installer to quickly install an ACE instance on multiple computers.

Install an ACE Instance on a Single Windows Host

If VMware Player is not already installed on the machine, the installation program installs it before installing the virtual machine files that make up the ACE instance.

Before you begin, consider the following prerequisites:

- Make sure the host computer has enough disk space for the ACE instance.

- If this is the first installation of an ACE instance on the user machine, a user with administrative privileges must run the installation. Only a user with administrative privileges can install and uninstall VMware Player.
- If the ACE instance includes a host policy, a user with administrative privileges must run the installation. A host policy is a host network access policy or a policy that restricts which virtual machines can run on a host. See [“Setting Network Access Policies”](#) on page 384 and [“Control Which ACE Instances Run on a Host”](#) on page 401.

Only one set of host policies can be deployed to a particular host. If a package contains host policies and the host already contains host policies from another package, installation of the second package fails.

To install an ACE instance on a single Windows host

- 1 If VMware Player is not yet installed on the user's machine, log in to the host computer as the Administrator user or as a user who is a member of the Windows Administrators group.
- 2 Depending on whether you are installing from a CD, DVD, or network location, do one of the following:
 - For CDs and DVDs, insert the first disc.
 - For a network location, navigate to the location of the installer.
- 3 Find the `setup.exe` file and double-click it.
- 4 Follow the instructions in the installation wizard.

Install an ACE Package Silently on Multiple Windows Hosts

If you are installing a VMware ACE package on a number of Windows host computers, you might want to use the silent installation features of the Microsoft Windows Installer. This type of installation requires that the host computers have version 2.0 or later of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP. If the runtime engine is not installed, see [“Install the MSI 2.0 Runtime Engine from an ACE Package”](#) on page 442.

Install the MSI 2.0 Runtime Engine from an ACE Package

The installer for the MSI 2.0 runtime engine is included in the VMware ACE package as the `instmsiw.exe` file.

To install the MSI 2.0 runtime engine from an ACE package

- 1 On the host computer, open a command prompt.
- 2 Enter the following command:

```
instmsiw.exe /Q
```

For additional details on how to use the Microsoft Windows Installer, see the Microsoft Web site.

Install an ACE Instance on Multiple Hosts

You can use the Microsoft Windows Installer command-line interface to silently install an ACE instance on many computers. End users are not prompted for information during the installation process.

You can customize the basic package installation command to specify one or more of the following:

- Installation directory for the ACE instance
- Installation directory for VMware Player
- Installation without a desktop icon

You can also install an upgrade silently. An upgrade is always installed in the same directory or directories as the previous package.

To install the ACE instance on multiple hosts

- 1 On the host computer, open a command prompt.
- 2 Enter the following command:

```
setup.exe /s/v"/qn"
```

This command installs the package and VMware Player (if included) into the default locations and creates a shortcut for the ACE instance on the desktop. The default location for the VMware Player application is C:\Program Files\VMware\VMware Player.

The default location for the virtual machine files on a Windows XP system is C:\Documents and Settings\All Users\Application Data\VMware\VMware ACE\<ACE_name>.

- 3 To customize the package, enter the following command:

```
msiexec -i package.msi <installation_options>
```

Enter the command on one line. The installation options follow.

Option	Description
DESKTOP_SHORTCUTS	When set to 0, skips installation of the ACE instance shortcut on the desktop. The default is 1.
INSTALLDIR	Sets the root installation directory for the ACE instance.
PLAYER_INSTALLDIR	Sets the root installation directory for the VMware Player application.

The following example command illustrates the options and their usage:

```
msiexec -i package.msi DESKTOP_SHORTCUTS=0
INSTALLDIR="G:\packages"
PLAYER_INSTALLDIR="C:\VMware\VMware Player" /qn
```

Uninstall VMware Player or an ACE instance from a Windows Host

Uninstalling VMware Player does not uninstall the ACE instance. Only the Administrator user or a user who is a member of the Windows Administrators group can uninstall VMware Player.

Uninstalling an ACE instance does not uninstall the VMware Player application. When you remove an ACE instance, the ACE instance's data files, shortcuts, and registry entries are removed. You do not need to be an Administrator user to uninstall an ACE instance.

To uninstall VMware Player or an ACE instance from a Windows host

- 1 Go to **Start > Control Panel > Add or Remove Programs > Change or Remove Programs**.
- 2 Select the VMware Player program or the ACE instance and click **Remove**.
- 3 Follow the instructions in the wizard.

Installing an ACE Package on a Linux Host

If an end user's computer does not already have VMware ACE or VMware Player installed, the first time you install an ACE package, VMware Player is installed along with the ACE instance. If VMware Player is not already installed on the machine, it is automatically installed when you run the ACE package's `vmware-install.pl` as root or sudo.

You can install ACE instances on one host at a time, or you can silently install an ACE instance on multiple computers.

Manually Install VMware Player on a Linux Host

Manually install VMware Player on systems where the end user does not have root access.

To manually install VMware Player on a Linux host

- 1 In a terminal window, enter the following command to become the root user:

```
su -
```

- 2 Mount the ACE package, and locate the VMware Player installer in the package directory.

Depending on whether the host is a 32-bit computer or a 64-bit computer, you see one of the following filenames:

- **VMware-player-i386.tar.gz**
- **VMware-player-x86_64.tar.gz**

- 3 Copy the tar archive to a temporary directory on the hard drive.

For example, if you have a 64-bit computer and you want to put the file in the `/tmp` directory, enter the following command:

```
cp VMware-player-x86_64.tar.gz /tmp
```

- 4 Enter the following command to change to the directory to which you copied the file:

```
cd /tmp
```

- 5 Enter one of the following commands to unpack the archive:

- **tar xzf VMware-player-i386.tar.gz**
- **tar xzf VMware-player-x86_64.tar.gz**

- 6 Enter the following command to change to the installation directory:

```
cd vmware-player-distrib
```

- 7 Enter the following command to run the installation program:

```
./vmware-install.pl
```

- 8 Accept the default directories for the binary files, library files, manual files, documentation files, and the initiation script.
- 9 Select **Yes** when prompted to run the `vmware-config.pl` file and accept the default values for the remaining prompts.

If you do not enable host-only networking when you install VMware Player, you cannot allow a virtual machine to use both bridged and host-only networking.

- 10 When installation is completed, enter the following command to exit from the `root` account:

```
exit
```

Install the ACE Instance on a Single Linux Host

Only the user who installs the ACE instance or a user with necessary permissions (such as `root`) is allowed to run that ACE instance. If VMware Player is not already installed on the machine, it is automatically installed when you run the ACE package's `vmware-install.pl` as `root` or `sudo`.

Before you begin, consider the following prerequisites:

- Make sure the host computer has enough disk space for the ACE instance.
- The ACE package must be accessible to the Linux user machines for installation.
- If this is the first installation of an ACE instance on the user machine, a root user must run the installation. Only a root user can install and uninstall VMware Player.
- If the ACE instance includes a host policy, a root user must run the installation. A host policy is a host network access policy or a policy that restricts which virtual machines can run on a host. See [“Setting Network Access Policies”](#) on page 384 and [“Control Which ACE Instances Run on a Host”](#) on page 401.

Only one set of host policies can be deployed to a particular host. If a package contains host policies and the host already contains host policies from another package, installation of the second package fails.

To install an ACE instance on a single Linux host

- 1 Open a terminal window and change to the package directory.
- 2 Enter the following command:

```
vmware-install.pl
```

- 3 When prompted, select the directory in which you want to install the ACE instance.

Install an ACE Package Silently on Multiple Linux Hosts

You can silently install an ACE instance on many computers. End users are not prompted for information during the installation process.

To install the ACE instance on multiple Linux hosts

- 1 On the host computer, open a terminal window.
- 2 Enter the following command:

```
/tmp/<path_to_package>/ACE_Pkg/vmware-install.pl --default
```

This command installs the package and VMware Player (if included) into the default locations

Uninstall VMware Player or an ACE Instance from a Linux Host

ACE users can uninstall only the ACE instances that they installed. Only the root user can uninstall others' ACE instances. Uninstalling an ACE instance does not uninstall the VMware Player application. When you uninstall an ACE instance, the ACE instance's data files, shortcuts, and registry entries are uninstalled.

Uninstalling VMware Player does not uninstall the ACE instance. Only the root user can uninstall VMware Player.

To uninstall VMware Player or an ACE instance from a Linux host

- 1 On the host computer, open a terminal window.
- 2 Do one or both of the following:
 - To uninstall an ACE instance, enter the following command:

```
<path_to_instance_directory>/vmware-uninstall-ace.pl
```

- To uninstall VMware Player, enter the following command:

```
/usr/bin/vmware-uninstall.pl
```

Start and Use an ACE Instance

When you run an ACE instance, VMware Player starts and opens the instance. You start the instance in the same way that you start other applications on the host.

One exception is if the administrator configures the ACE instance to start and run in full screen mode when the host system starts. See [“Setting Runtime Preferences Policies”](#) on page 395.

Depending on how the ACE instance is configured, end users might be required to enter no password, one, or two passwords when they run the instance for the first time. The possibilities are:

- No passwords are required at the first run of the instance or on subsequent runs.

- You must enter one password at the first run, and that password is supplied to you by the administrator. On subsequent runs of the instance, no passwords are required.
- You must create a password at the first run. On subsequent runs, you must enter that password.
- You must enter an administrator-supplied password at the first run and also create a password. On subsequent runs, you must enter only the password that you created.

The administrator can also restrict how many characters or which characters can be used in passwords that end users create. See [“Authentication Settings”](#) on page 377.

To start and use an ACE instance

- 1 Depending on the host operating system, do one of the following:
 - On Windows hosts, use the desktop icon or the **Start** menu to start the ACE instance.
 - On Linux hosts, use the **Applications** menu or enter the following command in a terminal window:


```
vmplayer <path_to__package_directory>/<name_of_ACE_vmx_file>.vmx
```
- 2 If prompted to enter or create a password, do so.
- 3 If the Enter Serial Number dialog box appears, do one of the following:
 - If your administrator provided a serial number, enter it.
 - If you need to purchase a license, click **Get Serial Number**.
- 4 Click inside the VMware Player window to begin using the guest operating system and the applications installed in the ACE instance.

You can use the operating system and applications just as you would if they were running directly on a physical computer.
- 5 (Optional) To change a password that you created, choose **VMware Player > Change Password**.
- 6 (Optional) For more information about using VMware Player, choose **VMware Player > Help**.

Install an ACE Client License

An ACE client license is a device-specific license. Devices include PCs, laptops, and portable media devices such as USB flash drives (storing a Pocket ACE). The details of

the licensing terms are provided in the end user license agreement (EULA) for ACE published on www.vmware.com.

A licensed device can run any number of ACE instances. The ACE client license is associated with the device it is installed on and is not restricted to a specific ACE instance.

If you purchase a volume license, you do not need to install client licenses.

To install an ACE client license

- 1 Obtain the ACE client license serial number from your ACE administrator.
- 2 Double-click the desktop shortcut for the installed ACE instance.
- 3 At the prompt, enter the serial number in the appropriate field and enter your name and the organization name in the dialog box.
- 4 Click **OK**.

Change the ACE Client License

To change the ACE Client License

- 1 Choose **VMware Player > Enter ACE Client License**.
- 2 Do one of the following:
 - Enter the serial number in the dialog box.
 - If you need to purchase a license, click **Get Serial Number**.
- 3 Click **OK**.

Quit VMware Player

As a best practice, quit VMware Player before you shut down the host computer.

To quit VMware Player

Choose **VMware Player > Exit** on Windows hosts or **VMware Player > Quit** on Linux hosts.

Depending on the configured exit behavior, the ACE instance is suspended or shuts down and the window closes.

Also depending on the configuration, end users might be able to change the exit behavior in the Preferences dialog box (**Player > Preferences**).

Troubleshooting Tools

VMware ACE includes some troubleshooting tools that allow administrators and help desk assistants to fix some common problems that users have with ACE instances, such as forgotten user passwords. The tools are:

- For standalone ACE instances:
 - The ACE Tools, which is a command-line tool. See [“ACE Tools: vmware-acetool Command-Line Tool”](#) on page 450.
 - The hot fix feature, which users access from buttons in dialog boxes. See [“Respond to Hot Fix Requests”](#) on page 452.
- For managed ACE instances, see the *VMware ACE Management Server User's Guide*.

ACE Tools: vmware-acetool Command-Line Tool

The `vmware-acetool` command-line tool is a troubleshooting tool that enables ACE administrators to fix a limited set of problems for standalone ACE instances directly on an ACE user's system.

You can provide the following solutions with `vmware-acetool`:

- Set the user's password, so the user can run the ACE instance.
- Set copy protection, so the user can run the ACE instance in a new location.
- Set the expiration date, so the user can continue to use an ACE instance that is past its scheduled expiration date.

The configuration file (`.vmx` file) for the ACE instance must be on the ACE user's machine. That is, you cannot use `vmware-acetool` to make fixes to files associated with the instance unless the configuration file is on the same machine as those files.

You can actually use the `vmware-acetool` program to reset passwords and fix expiration dates on another machine, but you must have the `.vmx`, `.vmp1`, and `ace.dat` files from the user all set up in the same directory. The following is an example of a `vmware-acetool` command:

```
vmware-acetool <command> <ACEconfigurationfile> <parameters>
```

Command	Parameters	Description
<code>setPassword</code>	Path to recovery key file	Set the ACE instance's password.
<code>setExpirationDate</code>	New expiration date	Set the ACE instance's expiration date.

Command	Parameters	Description
allowCopy		Allow the ACE instance to run from its current location.
updateCurrentTime		Update the internal policy clock of an ACE instance to the current time.
cloneToVM	Net clone configuration file Path to recovery key file	Clone a regular virtual machine from an ACE-enabled virtual machine.

Password Prompts

All commands prompt for the administrative tools password. See [“Setting Administrator Mode Policies”](#) on page 399.

The `setPassword` command also prompts for the recovery key password for the private recovery key file, a new ACE instance password, and confirmation of that new password. See [“Set a Recovery Key for Encrypted ACE Instances”](#) on page 380.

Following is an example of the command:

```
vmware-acetool setPassword myACE.vmx recKey.priv
```

Expiration Dates

The new expiration date can be passed as one of the following:

- A number of days from the current date
- An absolute date in the format YYYY-MM-DD
- A start date and an end date in the format YYYY-MM-DD YYYY-MM-DD
- The special value "never", so that the instance never expires
- The special value "expired", so that the instance expires immediately

Following are examples of the command:

```
vmware-acetool setExpirationDate myACE.vmx 30
```

```
vmware-acetool setExpirationDate myACE.vmx 2007-06-16
```

```
vmware-acetool setExpirationDate myACE.vmx "never"
```

```
vmware-acetool allowCopy myACE.vmx 30
```

Respond to Hot Fix Requests

If you enable the hot fix feature for standalone ACE instances, users can easily request help to resolve the following problems:

- Lost or forgotten password
- Expired ACE instance
- Copy-protected ACE instance run from a new location

For information about enabling the hot fix feature, see [“Setting Hot Fix Policies for Standalone ACE Instances”](#) on page 400. For information about setting a recovery key, which you must have to send a hot fix for a lost or forgotten user password, see [“Set a Recovery Key for Encrypted ACE Instances”](#) on page 380.

When the hot fix feature is enabled, if an end user sees a notification that the ACE instance is expired or copy protected, a **Request Hot Fix** button appears in the dialog box. The user clicks this button, which launches the Hot Fix Request wizard. This wizard generates a hot fix request file. The user can submit this file to the administrator as an email attachment or in some other way.

To respond to a hot fix request

- 1 When you receive the hot fix request file, save it to a location that you can access from the administrator machine where Workstation is installed.
- 2 Open the ACE-enabled virtual machine for the instance that requires the hot fix.
- 3 Choose **File > Open**.
- 4 Navigate to the location of the hot fix request file and click **Open**.

A hot fix tab opens in the Workstation window. The hot fix tab displays the user's name and email address, the problem that led to the hot fix request, and any additional note the user entered.

- 5 Click **Approve hot fix**.
- 6 Enter the appropriate information in the dialog box.
- 7 Select one of the following methods for sending the response:
 - Click **Send hot fix** on the hot fix tab and click **OK**.
 - Send the hot fix file. It is in the same folder as the hot fix request. The file extension for the fix file is `.vmhf`.

The display on the hot fix tab shows the status of the hot fix request, approved or denied, and the date on which you took action.

The user applies the hot fix by double-clicking the hot fix file.

Troubleshooting Setup Issues

Occasionally ACE end users have problems logging in to a domain after running the **Revert to Reimage Snapshot** command. They might sometimes also have problems with domain validation and name resolution.

Login Issues After Reverting to a Reimage Snapshot

Problem: The ACE user can't log the ACE instance back in to a domain after choosing **VMware Player > Troubleshoot > Revert to Reimage Snapshot**.

Description: The ACE instance has a Windows guest operating system installed and the machine account password for the domain is periodically renewed by default. If the password is renewed by the time the user reverts the ACE instance to the snapshot, the snapshot's password is invalid and login fails.

Solution: To avoid this problem, ensure that the following security policy is enabled: **Refuse machine account password changes**.

You can enable this policy on the ACE-enabled virtual machine (affecting all instances created from it) or on the primary domain controller. For details about how to change the policy, see the following Microsoft articles:

- Local Security Policies – Go to the Microsoft Support site, enter the Microsoft knowledge base article ID 175468 in the search criteria, and click on the first search result.
- PDC Security Policies – Go to the Microsoft TechNet site and enter Domain controller: Refuse machine account password changes, in the search criteria. Issues with Domain Validation or Name Resolution

Problem: When you try to join an ACE-enabled virtual machine to a domain, domain validation or name resolution does not work.

Description: Some ACE-enabled virtual machines with certain network configurations might demonstrate these problems.

Solution: Consult the Microsoft knowledge base article. Go to the Microsoft Support site, enter the Microsoft knowledge base article ID 314108 in the search criteria, and click on the first search result.

Issues with Domain Joins for Windows Vista Guests

Problem: An ACE instance running under a Windows Vista guest operating system cannot join the local domain and that instance customization failed with the message "NetDomainJoin function Error 1722: Could not join domain."

Description: ACE instances running in the Windows Vista operating system might have this problem.

Solution: Tell the user to power off the instance and power it on again to retry instance customization. The problem is intermittent and restarting might solve the problem.

Beta

Workstation Command-Line Reference



This appendix discusses the command-line options that are available for the `vmware` program and the `vmrun` program. This appendix contains the following topics:

- [“Startup Options for Workstation and Virtual Machines”](#) on page 455
- [“Command-Line Application for Operating Virtual Machines”](#) on page 457

For information about using the `vmware-fullscreen` command to use full-screen switch mode, see [“Starting and Stopping Virtual Machines on a User’s Computer”](#) on page 361.

Startup Options for Workstation and Virtual Machines

[Table A-1](#) describes options available when you run VMware Workstation from the command line. You can type these commands in a Linux terminal window or at the Windows command prompt. You can also create scripts to run multiple commands.

The syntax for this command is:

- On a Linux host operating system:

```
/usr/bin/vmware [-n] [-x] [-X] [-m] [-t] [-q] [-s <variablename>=<value>]
                [-v]
                [/<path_to_virtual_machine>/<virtual_machine_name>.vmx]
                [X toolkit options]
```

- On a Windows host operating system:

```
C:\Program Files\VMware\VMware Workstation\Programs\vmware.exe [-B] [-n]
                    [-x] [-X] [-t] [-q] [-s <variablename>=<value>] [-v]
                    [<path_to_virtual_machine>\<virtual_machine_name>.vmx]
```

Table A-1. Command-Line Options for the vmware Program

Option	Description
-n	Opens a new Workstation window.
-B	(Windows hosts only) Opens a new Workstation window but hides the sidebar and toolbars. Only the tabs of open virtual machines are shown. Using this option has the same effect as clicking the Workstation icon in the upper-left corner of the Workstation window and choosing Hide Controls from the menu that appears.
-t	Opens a virtual machine or team in a new tab in the existing Workstation window.
-x	Powers on the virtual machine when VMware Workstation starts. This is equivalent to clicking the Power On button in the VMware Workstation toolbar.
-X	Powers on the virtual machine and switches the VMware Workstation window to full-screen mode.
-m	(Linux hosts only) Starts the program in quick switch mode.
-q	Closes the virtual machine's tab when the virtual machine powers off. If no other virtual machine is open, it also exits Workstation. This is useful when the guest operating system is capable of powering off the virtual machine.
-s	Sets the specified variable to the specified value. Any variable names and values that are valid in the configuration file may be specified on the command line with the -S switch.
-v	Displays the product name, version, and build number.
<path_to_virtual_machine ><path_to_virtual_team>	Launches a virtual machine using the specified virtual machine or team configuration file (.vmx or .vmtm file).

On Linux hosts, X toolkit options can be passed as arguments, although some of them (most notably the size and title of the VMware Workstation window) cannot be overridden.

X toolkit options are not relevant on a Windows host.

Using Startup Options in a Windows Shortcut

The most convenient way to use the startup options is to incorporate them into the command generated by a Windows shortcut.

To create the shortcut, right-click the shortcut and click **Properties**. In the **Target** field, add any switches you want to use after the `vmware.exe` filename. For example, the

following command launches the Windows Me virtual machine specified, powers it on, and switches to full-screen mode.

```
"C:\Program Files\VMware\VMware Workstation\Programs\vmware.exe -X
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\Windows Me\Windows Me.vmx"
```

Enclose the entire command string in quotation marks.

NOTE The configuration file has a .vmx extension by default.

Command-Line Application for Operating Virtual Machines

VMware Workstation includes a separate application, `vmrun`, for operating teams or virtual machines from the command line. Before using the `vmrun` command on a Windows host, you must do one of the following:

- Change your working directory to the VMware Workstation directory. The default location is:

```
c:\Program Files\VMware\VMware Workstation
```

- Add the VMware Workstation directory to the system path. On Windows 2000 and XP, you can change this setting at

Control Panel>System>Advanced>Environment Variables>System variables>Path

To launch the `vmrun` application, from the command prompt, enter: **`vmrun` COMMAND [OPTION]**.

Valid `vmrun` commands and options are described in [Table A-2](#).

If authentication is required in the guest operating system, use the following authentication flags, as appropriate:

```
-gu <userName in guest OS>
-gp <password in guest OS>
```

Table A-2. `vmrun` Commands and Parameters

Command	Description	Parameters
General Commands		
<code>list</code>	List all running virtual machines.	None
<code>upgrademv</code>	Upgrade a virtual machine to the current Workstation version.	[Path to .vmx file]

Table A-2. vmrun Commands and Parameters (Continued)

Command	Description	Parameters
installtools	Install VMware Tools in the guest operating system. In Windows guests, the VMware Tools installer runs automatically. In Linux guests, this command connects the virtual machine's virtual CD-ROM drive to the VMware Tools ISO image for that guest, but the installer does not start automatically. Complete the installation with additional manual steps, as described in “Install VMware Tools on a Linux Guest Within X by Using the RPM Installer” on page 110.	[Path to .vmx file]
Power Commands		
start	Start a virtual machine (.vmx file) or team (.vmtm file).	[Path to .vmx or .vmtm file]
stop	Stop a virtual machine (.vmx file) or team (.vmtm file). Use the <code>soft</code> parameter to shut down the guest. Use the <code>hard</code> parameter to power it off as if you pressed the power button.	[Path to .vmx or .vmtm file] [<code>hard</code> <code>soft</code>]
reset	Reset a virtual machine (.vmx file) or team (.vmtm file). Use the <code>soft</code> parameter to shut down the guest before restarting. Use the <code>hard</code> parameter to power it off as if you pressed the power button.	[Path to .vmx or .vmtm file] [<code>hard</code> <code>soft</code>]
suspend	Suspend a virtual machine (.vmx file) or team (.vmtm file). Use the <code>soft</code> parameter to release the IP address (on Windows guests) or stop networking (on UNIX guests) before suspending.	[Path to .vmx or .vmtm file] [<code>hard</code> <code>soft</code>]
Snapshot Commands		
snapshot	Create a snapshot of a virtual machine.	[Path to .vmx file] [snapshot name]
listSnapshots	List all snapshots in a virtual machine.	[Path to .vmx file]
deleteSnapshot	Remove a snapshot from a virtual machine.	[Path to .vmx file] [snapshot name]

Table A-2. vmrun Commands and Parameters (Continued)

Command	Description	Parameters
revertToSnapshot	<p>Go to a snapshot in a virtual machine.</p> <p>If a snapshot has a unique name within a virtual machine, revert to that snapshot by specifying the path to the virtual machine's configuration file and the snapshot name: [Path to .vmx file][snapshot name]</p> <p>If several snapshots have the same name, you can still specify a snapshot by including a "path name" for the snapshot name. A path name is a series of snapshot names, separated by forward slash characters (/). Each name specifies a different snapshot in the tree.</p> <p>For example, suppose you include the path name Snap1/Snap2. This will identify a snapshot named Snap2 that was taken from the state of a root snapshot named Snap1.</p> <p>Because you can use the forward slash in a path name, VMware recommends that you avoid using the slash character when you name a snapshot because this makes it difficult for you to predict which snapshot a path name will identify.</p>	<p>[Path to .vmx file] [snapshot name] or [Path to .vmx file] [snapshot name1/ snapshot name2]</p>
Guest Operating System Commands		
runProgramInGuest	Run a program in the guest operating system.	<p>[Path to .vmx file] [Program [Program arguments]]</p>
fileExistsInGuest	Check whether the specified file exists in the guest system.	<p>[Path to .vmx file] [Path to file in guest]</p>
setSharedFolderState	Modify the location of a folder shared between the host and guest.	<p>[Path to .vmx file] [Share name] [New path to folder on host]</p>
addSharedFolder	Add a folder to be shared between the host and guest.	<p>[Path to .vmx file] [Share name] [Path to folder on host]</p>
removeSharedFolder	Remove a folder shared between the host and guest.	<p>[Path to .vmx file] [Share name]</p>
listProcessesInGuest	List the processes running in the guest operating system.	[Path to .vmx file]

Table A-2. vmrun Commands and Parameters (Continued)

Command	Description	Parameters
killProcessInGuest	Kill the specified process on the guest operating system.	[Path to .vmx file] [Process ID]
runScriptInGuest	Run a script in the guest operating system.	[Path to .vmx file] [Interpreter path script text]
deleteFileInGuest	Delete a file from the guest operating system.	[Path to .vmx file] [Path to file on the guest]
createDirectoryInGuest	Create a directory in the guest operating system.	[Path to .vmx file] [Directory path on the guest]
deleteDirectoryInGuest	Delete a directory from the guest operating system.	[Path to .vmx file] [Directory path on the guest]
listDirectoryInGuest	List the contents of a directory in the guest operating system.	[Path to .vmx file] [Directory path on the guest]
copyFileFromHostToGuest	Copy a file from the host to the guest operating system.	[Path to .vmx file] [File path on the host] [File path on the guest]
copyFileFromGuestToHost	Copy a file from the guest operating system to the host.	[Path to .vmx file] [File path on the guest] [File path on the host]
renameFileInGuest	Rename a file in the guest operating system.	[Path to .vmx file] [Original file name] [New file name]

Examples for vmrun

For example, to reset a virtual machine:

- In a Linux terminal, enter:

```
vmrun reset /usr/local/VMs/<virtual_machine_name>.vmx soft
```

- On the Windows command line, enter:

```
vmrun reset c:\Virtual Machines\<virtual_machine_name>.vmx soft
```

With virtual machines that require input through a VMware Workstation dialog box, `vmrun` might time out and fail. To disable Workstation dialog boxes, insert the following line into the configuration (`.vmx`) file for a virtual machine:

```
msg.autoAnswer = TRUE
```

BETA

BETA

Using the Eclipse Integrated Virtual Debugger



This appendix contains the following sections:

- [“Installation Requirements for the Eclipse Integrated Virtual Debugger Environment”](#) on page 464
- [“Managing Virtual Machine Launch Configurations”](#) on page 469
- [“Running and Debugging Applications in Virtual Machines”](#) on page 472

The Eclipse Integrated Virtual Debugger provides a configurable interface between Eclipse and virtual machines, making it easy to develop and debug applications that run in multiple operating system environments on a single PC. Debugging your applications in virtual machines enables you to reproduce and record errors while maintaining the integrity of the host machine.

You can perform typical debugging tasks such as pausing at breakpoints, stepping through code, and viewing and modifying the state of your application, all without impacting the host environment. The Eclipse Integrated Virtual Debugger also enables you to:

- Manage launch configuration settings for application execution and debugging in virtual machines.
- Start an application debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Using Eclipse launch configurations, you can choose a virtual machine in which to run your application and how it is execute. When configured, the Eclipse Integrated Virtual

Debugger finds the virtual machine, powers it on if necessary, sets up the environment based on your configuration settings, and starts or attaches to the application.

To configure how an application is started in a virtual machine, you can specify:

- Name of the virtual machine (.vmx configuration file).
- Account credential for guest console
- (Optional) Path to the Java Virtual Machine (JVM) on the guest system.
- (Optional) Locations of folders to be shared between the host and the guest.
- (Optional) Actions to perform before launching an application from Eclipse, including:
 - Revert to the most recent snapshot.
 - Run specified pre-execution commands.
- (Optional) Actions to perform after an application launched from Eclipse is terminated, including:
 - Run specified post-execution commands (for example, to perform cleanup tasks).
 - Set the virtual machine state to:
 - Suspended (default)
 - Revert to the most recent snapshot
 - Powered off

Installation Requirements for the Eclipse Integrated Virtual Debugger Environment

Review the requirements and recommendations in this section before following the instructions in [Chapter 2, “Installing VMware Workstation,”](#) on page 39 to install the Eclipse Integrated Virtual Debugger as an optional component of Workstation 6.5. This section describes the requirements for host and guest systems, Eclipse, and the Java Runtime Environment (JRE).

During Windows installation, if Eclipse is not installed in C:\Program Files\Eclipse or C:\Eclipse, you must use the **Custom** setup to select the Eclipse Integrated Virtual Debugger component and specify the Eclipse directory location.

During Linux installation, you must override the default value of **No** when prompted by `vmware-config.pl` to install the Eclipse Integrated Virtual Debugger.

When you install the Eclipse Integrated Virtual Debugger:

- The Eclipse Integrated Virtual Debugger plug-in, `ivd.jar`, Foundry Java bindings, and the `plugin.xml` launch configuration file are placed in the `com.vmware.bfg_1.0.0` subdirectory of the Eclipse plug-in directory.
- After you restart Eclipse, the **Debug** menu includes the new launch configuration types **VMware attach to application** and **VMware execute Java application**. These launch configuration types have a **VMware** tab that enables you to configure virtual machine settings.

You can debug in multiple virtual machines simultaneously. You can also debug multiple sessions in a single virtual machine.

Host System Requirements

The Eclipse Integrated Virtual Debugger can run on any supported host operating system that is running Workstation 6.5 and has Eclipse installed. Eclipse must be running on the same system as Workstation 6.5. For more information about, see [“Eclipse Requirements”](#) on page 466.

Supported Host Operating Systems

The Eclipse Integrated Virtual Debugger supports the following Windows 32-bit, Linux 32-bit, and Linux 64-bit host operating systems.

Table B-1. Windows and Linux Host Operating Systems

Operating System	Edition
Windows 32-bit	Windows Vista Enterprise
	Windows Vista Business
	Windows Vista Home Basic and Premium
	Windows Vista Ultimate
	Windows XP Home Edition, SP1, SP2
	Windows XP Professional, SP1, SP2
	Windows 2000 Server SP3, SP4
	Windows 2000 Professional, SP3, SP4
	Windows 2000 Advanced Server, SP3, SP4

Table B-1. Windows and Linux Host Operating Systems (Continued)

Operating System	Edition
Linux 32 and 64-bit	Red Hat Enterprise Linux WS 4.5 (Beta, formerly called 4.0 Update 5)
	Red Hat Enterprise Linux AS 4.0, updates 1, 2, 3, 4
	Red Hat Enterprise Linux ES 4.0, updates 1, 2, 3, 4
	Red Hat Enterprise Linux WS 4.0, updates 1, 2, 3, 4
	Red Hat Linux 9.0 — stock 2.4.20-8, upgrade 2.4.20-20.9
	Ubuntu Linux 6.10 and 6.06

NOTE Windows 64-bit host operating systems are not currently supported.

Supported JRE Versions

The host system must be running a JRE meeting Java 2 Platform Standard Edition (J2SE) 5.0 or higher specifications. J2SE consists of the JRE and developer tools for compiling, debugging, and running applications written in the Java language.

NOTE Eclipse displays the error message `unable to load class` if an unsupported version of J2SE is being used on the host system.

Eclipse Requirements

You must have Eclipse 3.2 or 3.3 installed on the host. On Windows Vista hosts, you must have Eclipse 3.2.2 or 3.3 installed.

The Java language is supported. You cannot have GNU Compiler for the java programming language (GJC) installed on the guest operating system.

Virtual Machine Requirements

The Eclipse Integrated Virtual Debugger is supported on any Workstation 6.5 virtual machine that is running a supported Windows or Linux guest operating system.

Supported Guest Operating Systems

This section provides a simplified list of guest operating systems supported for debugging in virtual machines. For the most recent list of supported guest operating systems, including detailed information about the specific operating system versions,

service packs, and updates supported, see the *VMware Guest Operating System Installation Guide* at <http://pubs.vmware.com/guestnotes/>. This guide also provides notes on installing the most common guest operating systems.

NOTE Operating systems that are not listed are not supported for debugging in a virtual machine.

The Eclipse Integrated Virtual Debugger supports the following Windows 32-bit, Windows 64-bit, Linux 32-bit, and Linux 64-bit guest operating systems.

Table B-2. Windows and Linux Guest Operating Systems

Processor Type	Operating System Edition
Windows 32-bit	Windows Vista (all editions except Vista Home Edition, which cannot be run in a virtual machine due to Microsoft licensing restrictions.)
	Windows Server 2003 Enterprise Edition and R2
	Windows XP Professional and Home Edition
	Windows 2000 Professional
	Windows 2000 Server
	Windows 2000 Advanced Server
Windows 64-bit	Windows Vista x64 Edition (3-D effects not yet supported)
	Windows Server 2003 x64 Edition
	Windows XP Professional x64
Linux 32 and 64-bit	Red Hat Linux 8 and 9
	Red Hat Enterprise Linux Advanced Server Enterprise Server Workstation 4 and 5
	Ubuntu Linux 6.10 and 6.06
	SUSE Linux 10
	SUSE Linux Enterprise Server 10

VMware Tools Requirements

Make sure that the version of VMware Tools on the guest operating system matches the version of Workstation 6.5 (of which the Eclipse Integrated Virtual Debugger is a component) on the host.

Update Requirements for Java and JRE

You cannot have GCJ installed on the guest operating system.

The guest operating system must be running JRE 1.4.2 or higher. If you are not using JRE 5.0 on the guest, you must update the build settings in Eclipse to use a 1.4.x JRE on the guest.

To update the Eclipse build settings to use a 1.4.x JRE on the guest

- 1 In the Eclipse Package Explorer, right-click the topmost folder (Project item) and choose **Properties**.
- 2 In the left pane of the Properties page, select **Java Compiler**.
- 3 Select **Enable project specific settings**, and set the Java Development Kit (JDK) Compliance Compiler compliance level to **1.4**.

Installing PSAPI.DLL on Windows NT

On Windows NT, you must install the `psapi.dll` library file to retrieve process status information so that the Eclipse Integrated Virtual Debugger can attach to a process. You can download `psapi.dll` from

<http://msdn2.microsoft.com/en-us/library/ms684884.aspx>.

Disabling the Firewall on Linux Guest Systems

You must disable the firewall on Linux guest operating systems. The Eclipse Integrated Virtual Debugger opens an available port (searching from port 49152) for each debugging session.

Configure the Firewall on Windows Guest Systems

If you are using a 1.4.x JRE on Windows guest systems, you must either disable the firewall or allow incoming connections to the JVM. If your Windows system (such as Windows XP SP2, Windows 2003, and Windows Vista) allows you to configure exceptions to the firewall, you can add the JVM to the exceptions list.

To add the JVM to the exceptions list

- 1 Choose **Start > Control Panel > Windows Firewall** and select the **Exceptions** tab.
- 2 Click **Add Program** and browse to the Java executable.
- 3 Click **OK**.
- 4 (Optional) On Windows Vista guests, you might have to restart the firewall after configuring it to allow incoming connections to the JVM.

Managing Virtual Machine Launch Configurations

You can manage configuration settings for each virtual machine in which you want to debug applications. Eclipse Integrated Virtual Debugger launch configurations determine which virtual machine to run the application in and how the application is executed.

The launch configuration types **VMware attach to application** and **VMware execute Java application** have a **VMware** tab. The values you enter in the **VMware** tab determine virtual machine configuration settings. Once configured, you can start and attach to applications in virtual machines from the Eclipse **Debug** and **Run** menus.

Use Application Configurations to Start Applications in a Virtual Machine

This section describes how to create, duplicate, or edit a launch configuration to start an application in a virtual machine.

To create, duplicate, or edit a launch configuration to start an application in a virtual machine

- 1 Choose **Run > Debug**.

The **Debug** page is displayed. You can create, manage, and run configurations from this page.

- 2 You can create a launch configuration based on default settings or based on another configuration. You can also edit an existing configuration. Do one of the following:
 - Create a configuration based on default settings by selecting **VMware execute Java application** in the left pane, and clicking the **New launch configuration** icon at the top of the pane.
 - Create a configuration based on another configuration by selecting the configuration you want to duplicate under **VMware execute Java application** in the left pane, and clicking the **Duplicates the currently selected configuration** icon at the top of the pane.
 - Edit an existing configuration by selecting the configuration you want to edit under **VMware execute Java application** in the left pane.
- 3 Perform the remaining steps in the **VMware** tab of the right pane.
- 4 Choose a virtual machine from the drop-down menu of recently used and currently running virtual machines.

Click **Browse** to select from .vmx files on the system.

- 5 Enter your account credentials to access the guest console.
- 6 (Optional) If you want to use a JVM other than the one that is automatically selected, select an alternate JVM path.
- 7 (Optional) Expand the list of shared folders to add, edit, or remove folders to be shared between the host and the guest systems.

For each folder, enter the share name and the location on the host system.

By default, the project folder is shared.

- 8 (Optional) Indicate actions to be performed before the application is launched:
 - Select **Set virtual machine state to most recent snapshot** to revert to the most recent snapshot before the application is launched.
 - Select **Run script** and enter one or more shell commands to be executed in the guest operating system before the application is launched. No syntax checking is performed. Either enter one command per line, or enter multiple commands on the same line using a semicolon as a separator.
- 9 (Optional) Indicate actions to be performed after the application has terminated:
 - Select **Run script** and enter one or more shell commands to be executed in the guest operating system after the application has terminated. No syntax checking is performed. Either enter one command per line, or enter multiple commands on the same line using a semicolon as a separator.
 - Select **Set virtual machine state**, and select one of the following options to:
 - **Suspended** (default)
 - **Most recent snapshot**
 - **Powered-off**

- 10 Click **Apply**.

If you click **Revert**, settings revert to previous values.

If newly created, the launch configuration is added to the left pane.

Use Application Configurations to Attach to Applications Running in a Virtual Machine

This section describes how to create, duplicate, or edit a configuration that attaches to a running application in a virtual machine.

To create, duplicate, or edit a configuration that attaches to a running application in a virtual machine

- 1 Choose **Run > Debug**.

The **Debug** page appears. You can create, manage, and run configurations from this page.

- 2 You can create a launch configuration based on default settings or based on another configuration. Do one of the following:
 - Create a configuration based on default settings by selecting **VMware attach to application** in the left pane, and clicking the **New launch configuration** icon at the top of the pane.
 - Create a configuration based on another configuration by selecting the configuration you want to duplicate under **VMware attach to application** in the left pane and clicking the **Duplicates the currently selected configuration** icon at the top of the pane.
 - Edit an existing configuration by selecting the configuration you want to edit under **VMware attach to application** in the left pane.

Perform the remaining steps in the **VMware** tab of the right pane.

- 3 Choose a virtual machine from the drop-down menu of recently used and currently running virtual machines.

Click **Browse** to select from .vmx files on the system.

- 4 Enter your account credentials to access the guest console.
- 5 Click **Apply**.

If you click **Revert**, settings revert to default values.

If newly created, the launch configuration is added to the left pane.

Delete Configurations

To remove a configuration

- 1 Choose **Run > Debug**.

The **Debug** page is displayed. You can create, manage, and run configurations from this page.

- 2 In the left pane, select one or more configurations you want to delete and click the **Delete selected launch configuration(s)** icon at the top of the pane.

The configuration is removed in the left pane.

Running and Debugging Applications in Virtual Machines

After you create the appropriate launch configurations, the Eclipse Integrated Virtual Debugger enables you to:

- Start an application debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Start an Application Debugging Session in a Virtual Machine

.Do not suspend a virtual machine while the Eclipse Integrated Virtual Debugger is connected to an application. If you do, the Eclipse Integrated Virtual Debugger disconnects from the application.

To start a debugging session in a virtual machine

- 1 Begin the session in one of the following ways:
 - From the **Debug** menu, choose the configuration for the application to start debugging.
 - In the **Debug** page, select the configuration under **VMware execute Java application** in the left pane and click **Debug** in the right pane.
- 2 Perform debugging tasks as you would in a local debugging environment.

Start an Application in a Virtual Machine Without Debugging

You can start an application without debugging in any configured virtual machine. Begin the session in one of the following ways:

- From the **Run** menu, choose the configuration for the application to start.
- In the **Run** page, select the configuration under **VMware execute Java application** in the left pane and click **Run** in the right pane.

Attach the Debugger to an Application Running in a Virtual Machine

Do not suspend a virtual machine while the Eclipse Integrated Virtual Debugger is connected to an application. If you do, the Eclipse Integrated Virtual Debugger will disconnect from the application.

To attach to an application that is running in a virtual machine

- 1 In the **Debug** page, select the configuration under **VMware attach to application** in the left pane and click **Debug** in the right pane.

- 2 Select the process you want to attach to.

If more than one instance of the Java application is running in the virtual machine, a dialog box appears with a list of the running instances, each identified by their process ID, port number, and arguments.

- 3 Perform debugging tasks as you would in a local debugging environment.

BETA

Using the Visual Studio Integrated Virtual Debugger



This chapter contains the following sections:

- [“Setting Up the Visual Studio Integrated Virtual Debugger Environment”](#) on page 477
- [“Managing Virtual Machine Configurations”](#) on page 485
- [“Running and Debugging Applications in Virtual Machines”](#) on page 489

The Visual Studio Integrated Virtual Debugger provides a configurable interface between Visual Studio and virtual machines, making it easy to develop and debug applications that run in multiple Windows operating system environments on a single PC. Debugging your applications in virtual machines enables you to reproduce and record errors while maintaining the integrity of the host machine. You can perform typical debugging tasks such as pausing at breakpoints, stepping through code, and viewing and modifying the state of your application, all without impacting the host environment.

The Visual Studio Integrated Virtual Debugger enables you to:

- Manage configuration settings for application execution and debugging in virtual machines.
- Start an application debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

You can manage configuration settings for each virtual machine in which you want to execute and debug applications. Virtual machine configuration properties, which you

set in the Visual Studio Integrated Virtual Debugger configuration pages, determine which virtual machine to run the application in and how the application is executed.

Once configured, the integrated virtual debugger finds the virtual machine, powers it on if necessary, sets up the environment based on your configuration settings, and starts or attaches to the application.

Configuration Options When Starting an Application in a Virtual Machine

To configure how to start an application (with or without debugging) in a virtual machine, you can specify the following settings in the Visual Studio Integrated Virtual Debugger configuration pages:

- The command to be executed by Visual Studio in the guest operating system.
- The name of the virtual machine (.vmx configuration file).
- Whether to run the command as a shared path on the host or as a guest path.
- The location of the Remote Debug Monitor on the host.
- The name of the Remote Debug Monitor on the guest.

You can specify the following additional settings when you start debugging an application in a virtual machine, but not when you start an application without debugging:

- (Optional) The location of folders to be shared between the host and the guest.
- (Optional) Actions to perform before starting an application in a virtual machine, including:
 - Copying files or folders from the host to the virtual machine.
 - Reverting the virtual machine to the parent snapshot.
 - Running specified pre-execution commands on the guest. For example, if you must register new DLLs in the virtual machine each time the program is recompiled, you can create a DLL registration script and specify that it must be run during setup.
- (Optional) Actions to perform after an application in a virtual machine is terminated, including:
 - Running specified post-execution commands (for example, to perform cleanup tasks) in the guest.
 - Setting the virtual machine state to:

- No operation (remain powered on, no shutdown action)
- Powered off
- The parent snapshot
- Suspended

Configuration Options When Attaching to a Process Running in a Virtual Machine

To configure a debugging session that attaches to a process already running in a virtual machine, you can specify the following in the Attach to Process dialog box:

- The name of the virtual machine (.vmx configuration file).
- The location of the Remote Debug Monitor on the host.
- The name of the Remote Debug Monitor on the guest.

Setting Up the Visual Studio Integrated Virtual Debugger Environment

Review the requirements and recommendations in this section before following the instructions in [Chapter 2, “Installing VMware Workstation,”](#) on page 39 to install the Visual Studio Integrated Virtual Debugger as an optional component of Workstation 6.5. The Visual Studio Integrated Virtual Debugger can be installed on most Windows host systems that are running Workstation 6.5 and have a supported version of Visual Studio installed.

When you install the Visual Studio Integrated Virtual Debugger:

- The associated DLLs are placed in the \Program Files\VMware\VMware Workstation\Visual Studio Integrated Debugger and \Program Files\VMware\VMware VIX\ws-2\32bit directories.
- When you restart Visual Studio, the integrated virtual debugger is loaded and the **VMware** menu and toolbar become available.
- A preference file, vsid-prefs.xml, is created in the \Documents and Settings\<user_name>\Application Data\VMware directory. Do not edit this file directly. It is updated when you make changes in the integrated virtual debugger configuration pages.
- A file, <project_name>.idc, is created for each project in same directory as the project file when a project of a type supported by the integrated virtual debugger is loaded in Visual Studio.

- A log file, `vmware-vsld-<integer>.log`, is created in the `\Documents and Settings\<user_name>\Local Settings\Temp` directory. You can choose **VMware > About VMware Virtual Debugger** to view the log file name. This log file contains informational and error messages about the actions of the integrated virtual debugger.

When installed, you can debug in multiple virtual machines simultaneously. You can also debug multiple sessions in a single virtual machine.

NOTE However, you cannot debug on a local or physically remote machine and in a virtual machine at the same time.

Microsoft Visual Studio Requirements and Recommendations

This section includes requirements and configuration recommendations for Visual Studio.

Visual Studio must be running on the same system as Workstation 6.5.

Supported Versions of Visual Studio

Only Visual Studio 2005 Professional and Team Systems editions are supported. These versions of Visual Studio allow remote debugging on Windows systems, with the exceptions of Windows NT and Windows Vista Starter Edition. The Visual Studio Integrated Virtual Debugger uses the features of the Remote Debug Monitor (`msvsmon.exe`) to communicate with the guest operating system.

VMware recommends that you install Visual Studio 2005 SP1. For more information, see <http://msdn2.microsoft.com/en-us/vstudio/bb265237.aspx>.

For important information about running Visual Studio 2005 on Windows Vista, see <http://msdn2.microsoft.com/en-us/vstudio/aa972193.aspx>.

Running the Visual Studio Integrated Virtual Debugger on Windows Vista Starter Edition is not supported. For information about issues running Visual Studio on Windows Vista Starter Edition, see <http://msdn2.microsoft.com/en-us/vstudio/aa964140.aspx#question46>.

Supported Languages

The C/C++ (Native and Managed), C#, and Visual Basic languages are supported.

Configure the Runtime Library Setting for C++ Applications

When you debug on a physically remote machine or in a virtual machine, the application might not start if the runtime library setting is set to certain values. If you encounter this problem, change the C++ runtime library setting.

For additional information on C++ libraries, see <http://msdn2.microsoft.com/en-us/library/ms235624.aspx>.

To configure the Visual Studio runtime library setting

- 1 Choose **Project > Properties**.
- 2 Expand **Configuration Properties > C/C++** and select **Code Generation**.
- 3 Set **Code Generation** to **Runtime Library** property to **Multi-threaded (/MT)** or **Multi-threaded Debug (/MTd)**.

Host System Requirements

The Visual Studio Integrated Virtual Debugger can run on most Windows host operating systems supported by Workstation 6.5, listed in “32-bit” on page 28 and “64-bit” on page 29. On Windows Server 2003, only Enterprise Edition SP1 and R2 are supported.

If remote debugging is not working on a Windows Vista host, try the following:

- Manually configure the firewall to allow traffic from Visual Studio.
- Run Visual Studio with Administrator permissions. For more information, see <http://msdn2.microsoft.com/en-us/vstudio/aa972193.aspx>.

Virtual Machine Requirements and Recommendations

This section includes requirements and configuration recommendations for virtual machines.

Guest Operating System Support

The Visual Studio Integrated Virtual Debugger is supported on any Workstation 6.5 virtual machine that is running a supported Windows guest operating system. The operating systems that are not supported are:

- Windows NT
- Windows Me
- Windows 98

- Windows 95
- Windows for Workgroups
- Windows 3.1
- Windows XP Home Edition
- Windows Vista Starter Edition.

Make sure that the version of VMware Tools on the guest operating system matches the version of Workstation 6.5 (which the Visual Studio Integrated Virtual Debugger is a component of) on the host.

Configure the Network

Set up the virtual machine network as **Bridged** or **Host-only**. You cannot

To configure the network

- To configure the network on Windows XP, in the guest system:
 - Select **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options** page.
 - Set the policy **Network access: Sharing and security model for local accounts** to **Classic - local users authenticated as themselves**.
- To configure the network on Windows Vista, **Classic - local users authenticated as themselves** is the default value for this policy.

To verify that this policy is set correctly, follow the same steps as for Windows XP. It is not possible to view this policy on Windows Vista Home Premium and Vista Home Basic.

Configuring the Firewall on Windows XP SP2 Virtual Machines

Windows XP SP2 systems have the firewall enabled by default. To debug in a virtual machine with Windows XP SP2, you must disable the firewall or configure it appropriately. VMware recommends disabling the firewall. Virtual machines are protected behind the host firewall.

For information on setting up remote debugging in Visual Studio using Windows XP SP2 with the firewall enabled, see

<http://support.microsoft.com/default.aspx?scid=kb;%5BLN%5D;833977#2020>

Configuring User Accounts

Log in to the guest operating system with an Administrator account. Use the same local or domain user account on the host machine to log in to the guest operating system.

NOTE The user name, password, and domain name (if not local on both systems) must match on the host and the guest. Otherwise the Remote Debug Monitor on the guest will not be able to communicate with the Visual Studio debugger on the host.

For additional information on setting up Windows user accounts for remote debugging, see <http://msdn2.microsoft.com/en-us/library/ms164725.aspx>.

Communication between Visual Studio and the guest operating system is not initiated until the virtual machine is powered on and the configured user is logged in. The user runs the Remote Debug Monitor on the guest, which in turn communicates with the Visual Studio debugger on the host.

To prevent a time delay, power on the virtual machine and log in to the guest operating system before debugging in a virtual machine. You can set up automatic login to bypass the login screen when the guest is booting.

Setting the Password Policy

Windows has a default security feature that helps protect users with blank passwords from network-based attacks. Users who do not password-protect their accounts can log in only at their physical computer console: the monitor, keyboard, and mouse that is physically connected to their computer. This restriction applies only to local user accounts, not to domain user accounts.

For information on how to disable blank password restrictions, see <http://support.microsoft.com/?id=303846>.

Suppress Security Prompts

Running an application from a network share triggers a security prompt every time the file is accessed. VMware recommends that you turn off security prompts on the guest operating system.

To turn off security prompts on the guest system

- 1 In Internet Explorer, choose **Tools > Internet Options > Security > Local Intranet**, and click **Sites**.
- 2 Click **Advanced**, and add a new Web site:
`file://*..host`

Edit Registry Key to Suppress Security Prompts

To turn off security prompts by editing the registry key

- 1 Open the registry.
- 2 Add a new key, `.host`, under `HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Domains`.
- 3 In the `.host` key, create a new **DWORD Value** called `file` and set its value to 1.

Installing the Microsoft .NET Framework to Support Managed Applications

To debug managed C++, C#, and Visual Basic applications, which use the Common Language Runtime, you must install the Microsoft .NET Framework version 2.0 or higher on the guest operating system.

Rename Virtual Machine Computer Names

Verify that the computer names are unique on all virtual machines, otherwise the Visual Studio Integrated Virtual Debugger cannot find the appropriate virtual machine on the network.

To rename a computer

- 1 On the guest system, choose **Start > Control Panel > System**.
- 2 Select the **Computer Name** tab.
- 3 Click **Change**.
- 4 Type a unique name, and click **OK**.

Installing the Remote Debug Monitor Manually on Windows 98 Guest Systems

To enable debugging in a virtual machine, the Visual Studio Integrated Virtual Debugger shares the host folder that contains the Remote Debug Monitor, and runs that Remote Debug Monitor on the guest. On Windows 98, it is not possible to run the Remote Debug Monitor (or any executable) from a shared folder. An attempt to do so generates the following error:

The remote debugger is not properly installed. On a Windows ME or Windows 98 computer, the debugger cannot be run off a file share. Run the remote debugger setup.

Instead, you must manually install and start the Remote Debug Monitor executable, `msvsmon.exe`, on the guest operating system before starting a debugging session. You can copy `msvsmon.exe` to the guest before starting the debug session, create a mapping to a network share with the host where `msvsmon.exe` is located, or install `msvsmon.exe` from the Visual Studio 2005 installation CD.

Start the Remote Debug Monitor Without Authentication on the Default Port

Running the Remote Debug Monitor on the guest system without authentication poses a security risk for that guest, it is recommended that you take a snapshot first and set **Revert to Parent Snapshot to Yes** in **Post-Debug Event** or **Pre-Debug Event** properties, as described in [“Setting Configuration Properties”](#) on page 486.

Due to shared folder limitations, you must also:

- Set **Run Command As** to a **guest path**. This property, which indicates how the command being executed by the debugger is run, is described in [“Set General Properties”](#) on page 486.
- Leave **Shared Directories** unset, because directories cannot be shared between the host and the guest. This property is described in [“Set Virtual Machine Properties”](#) on page 487.

To start the Remote Debug Monitor without authentication on the default port

- 1 Run the command:


```
msvsmon.exe /noauth
```
- 2 Verify that you are using port 4015 by confirming that Remote Debug Monitor displays the following message:


```
Msvsmon started a new server named '<guest_name>:4015'.
Authentication is disabled. Waiting for new connections.
```

Troubleshooting Tips

This section contains additional information that enables you to use the Visual Studio Integrated Virtual Debugger successfully.

Changing Shortcut Keys

If you change the shortcut keys for VMDebugger commands (in **Tools > Options > Keyboard**), the tooltips for the VMware menu and toolbar will not reflect the changes until you restart Visual Studio.

Reinstalling VMware Tools If the Debugging Session Does Not Start

If the debugging session fails to start and the last message in the VMware output window (and log file) is **Waiting for VMware Tools to start**, check whether the guest system has the latest VMware Tools installed and running. If not, upgrade to the latest version of VMware Tools. See [“VMware Tools Update Process”](#) on page 117.

Exiting Visual Studio Before Powering Off a Virtual Machine

If you attempt to exit Visual Studio after starting a debugging session but before logging in or running VMware Tools on the guest, Visual Studio will not exit until the virtual machine is powered off or the user is logged in to the guest operating system.

Unloading the VMDebugger Add-in

To permanently uninstall the Visual Studio Integrated Virtual Debugger, run the Workstation installation program, select **Modify** on the Program Maintenance page, deselect **Visual Studio PlugIn** in the **Custom** setup, and continue through the installation wizard.

NOTE Deselecting **Start in Tools > Add-In Manager** does not prevent the Visual Studio Integrated Virtual Debugger Add-in from loading.

Clean Up After a Crash

If you try to run the debugger locally after a debugging session in a virtual machine crashes or freezes, you might get a Visual Studio error that indicates that the remote server cannot be found.

To reset Visual Studio and debug locally:

- In C++, choose **Project Property Pages > Debugging** and set the **Debugger to Launch** property to **Local Windows Debugger**.

Set the **Command** property to either an empty string or the correct local path.

- In C# and VB, choose **Project Property Pages > Debug**.

Make sure **Start project** is selected and **Use remote machine** is deselected.

- (Optional) You can remove any shared folders that were used to run the debug command and the Remote Debug Monitor. Shared folders are usually removed at the end of a debugging session, but they might not be removed in the following circumstances:

- If the debugging session causes a crash.

- If the virtual machine is powered off while the debugging session is still running.

These shared folders are typically reused when another debugging session is started, so this cleanup is not required.

Managing Virtual Machine Configurations

Before you can start or debug applications in a virtual machine, you must create or modify virtual machine configurations and set configuration properties. The default configuration initially includes the default values for all properties that have them.

Choose **VMware > Options** to manage configurations. You can create, rename, and remove configurations as described in this section, and you can set and modify configuration properties for existing configurations as described in [“Setting Configuration Properties”](#) on page 486.

The configuration selected in the **Configuration** drop-down menu is the one being edited in the configuration pages, while the configuration selected in the **Active Configuration** drop-down menu is the one used when you choose **VMware > Start** or **VMware > Start Without Debugging**.

Create Configurations

To create a new configuration

- 1 Choose **VMware > Options**.
- 2 Click the **New** icon next to the **Configuration** drop-down menu.
- 3 In the New Configuration page, type a name for the new configuration.
- 4 Choose a configuration to copy settings from.
- 5 The default selection is **<Default>**, which includes the default values for all properties that have them.
- 6 Click **OK**.

The new configuration is created and listed as the active configuration in the **Configuration** and **Active Configuration** drop-down menus. You can start editing the configuration properties.

Setting Configuration Properties

You can edit configuration properties for a specific configuration by choosing the configuration name from the **Configuration** drop-down menu. You can also edit configuration properties for all configurations by choosing **All Configurations** from the **Configuration** drop-down menu.

The default configuration initially includes the default values for all properties that have them.

Set General Properties

General properties include:

- The command to be executed by Visual Studio in the guest operating system.
- How the command is run: as a path on the host in a shared folder or as a path on the guest.
- The location of the Remote Debug Monitor on the host.
- The name of the Remote Debug Monitor on the guest.

To set general properties

- 1 Choose **VMware > Options**, and select **General** in the left pane.
- 2 Set **Command** to the command to be executed by the debugger in the guest system.
- 3 Click **Browse** to select a path to the executable on the host file system.

The command directory is shared between the host and the guest.

- 4 Set **Run Command As** to indicate how the debug command is run: either as **a host path through a shared folder** or **a guest path**.

When **a host path through a shared folder** is selected, the folder where the command is located is shared before the debugging session is started. The command is executed from the shared folder, and when the debugging session ends, the folder is no longer shared. The name of the shared folder is `\\.\host\Shared Folders\$(ProjectName)<random_number>`.

When **a guest path** is selected, the command is executed from the specified path on the guest.

The default is **a host path through a shared folder**.

- 5 Set **Remote Debug Monitor** to the location of the Remote Debug Monitor on the host.

The default is the Visual Studio installed path, typically:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote Debugger\x86\
msvsmon.exe
```

- Use the default Remote Debug Monitor if you are debugging a 32-bit process in a 32-bit virtual machine.
- (Optional) If you want to debug a 32-bit process in a 64-bit virtual machine, use the Remote Debug Monitor:

```
\Program Files (x86)\Microsoft Visual Studio 8\Common7\IDE\Remote
Debugger\x86\msvsmon.exe
```

- (Optional) If you want to debug a 64-bit process in a 64-bit virtual machine, use the 64-bit Remote Debug Monitor:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote
Debugger\x64\msvsmon.exe
```

- 6 Type a name for the Remote Debug Monitor on the guest.

The default name is <user name>.

If a Remote Debug Monitor is already running on the guest, when the new connection is made between the Remote Debug Monitor on the guest and the Visual Studio debugger on the host, you are prompted to choose whether to connect to the one that is running or start another one with a different name.

Set Virtual Machine Properties

Virtual machine properties include:

- The path to the virtual machine file (.vmx file).
- (Optional) The location of any directories shared between the host and the guest.

To set virtual machine properties

- 1 Choose **VMware > Options**, and select **Virtual Machine** in the left pane.
- 2 Set **Virtual Machine** to the path to the virtual machine file (.vmx file).
Click **Browse** to select from .vmx files on the system.
- 3 (Optional) Set **Shared Folders** to a semicolon-delimited list of paired folder names in the form <shared_name>=<host_folder_name>.

Click **Browse** to enter share names and folder names using a dialog box.

(Optional) Set Pre-Debug Event Properties

Pre-Debug Event properties determine which actions are performed before the debug command is run. All of these settings are optional.

To configure actions to perform before beginning debugging

- 1 Choose **VMware > Options**, and select **Pre-Debug Event** in the left pane.
- 2 Set **Revert to Parent Snapshot** to **Yes** or **No**.

If set to **Yes**, the virtual machine reverts to its parent snapshot when the debugging session is started.

The default is **No**.

- 3 Set **Copy Files** to a semicolon-delimited list of paired file or directory names that are copied from the host to the guest machine in the form
<host_machine_file/folder>=<virtual_machine_file/folder>.

Click **Browse** to select from files on the system.

All specified files are copied before any pre-debugging commands are executed.

- 4 Set **Command Line** to one or more semicolon-delimited commands that are run after files are copied (as described in the preceding step) and before the debugging session starts.

Click **Browse** to enter commands using a dialog box.

(Optional) Setting Post-Debug Event Properties

Post-Debug Event properties determine which actions are performed after the debug command is terminated. All of these settings are optional.

To configure actions to perform after debugging has occurred

- 1 Choose **VMware > Options**, and select **Post-Debug Event** in the left pane.
- 2 Set **Command Line** to one or more semicolon-delimited commands that are run after the debugging session ends.
- 3 Click **Browse** to enter commands using a dialog box.
- 4 Set **Termination Mode** to:
 - No operation (default)
 - Power off
 - Revert to parent snapshot

- Suspend

Rename Configurations

To rename a configuration

- 1 Choose **VMware > Options**.
- 2 Choose the configuration you want to rename from the **Configuration** drop-down menu, and click the **Edit** icon.
- 3 In the Edit Configuration page, select the configuration you want to rename, and click **Rename**.
- 4 Type the new name over the existing name, and press **Enter**.
- 5 At the confirmation prompt, click **Yes**.
- 6 Click **Close**.

The renamed configuration is listed as the active configuration in the **Configuration** drop-down menu. You can edit its configuration properties, as described in [“Setting Configuration Properties”](#) on page 486.

Remove Configurations

To remove a configuration

- 1 Choose **VMware > Options**.
- 2 Choose the name of the configuration you want to delete from the **Configuration** drop-down menu, and click the **Edit** icon.
- 3 In the Edit Configuration page, select the configuration you want to delete, and click **Remove**.
- 4 At the confirmation prompt, click **Yes**.
- 5 Click **Close**.

The configuration is removed from the **Configuration** drop-down menu.

Running and Debugging Applications in Virtual Machines

Once you have created the appropriate configurations, the Visual Studio Integrated Virtual Debugger enables you to:

- Start an application debugging session in a virtual machine.

- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Start a Debugging Session in a Virtual Machine

You can debug an application in any configured virtual machine.

NOTE You must log in to the guest system manually before the application is started. For additional information, see [“Configuring User Accounts”](#) on page 481.

To start a debugging session in a virtual machine

- 1 Choose **VMware > Start**.
The application is started in the virtual machine.
- 2 Perform debugging tasks as you would from the **Debug > Start Debugging** Visual Studio menu.
- 3 (Optional) If you want to kill the processes associated with the debugging session on the guest system and restart debugging, choose **VMware > Restart**.

Start a Session Without Debugging in a Virtual Machine

You can start an application in any configured virtual machine without debugging. When you start an application without debugging, the integrated virtual debugger does not execute pre-debug or post-debug operations, share additional directories, or start the Remote Debug Monitor on the guest system.

NOTE You must log in to the guest system manually before you can run the application. For additional information, see [“Configuring User Accounts”](#) on page 481.

To start an application in a virtual machine without debugging

- 1 Choose **VMware > Start Without Debugging**.
- 2 The Visual Studio Integrated Virtual Debugger initiates the following:
 - a Powers on the virtual machine if necessary.
 - b Shares the folder to the executable.
 - c Runs the executable.
 - d Removes the shared folder when the executable terminates.

- e Starts the application in the virtual machine.

Attach the Debugger to a Process Running in a Virtual Machine

To attach the debugger to a running process

- 1 Choose **VMware > Attach to Process**.

The Attach to Process page is displayed.

- 2 Choose the virtual machine on which to view running processes from the **Running Virtual Machines** drop-down menu.

Only virtual machines that are powered on appear in the drop-down menu.

- 3 Set **Remote Debug Monitor** to the location of the Remote Debug Monitor on the host.

The default is the Visual Studio installed path, typically:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote Debugger\x86\
msvsmon.exe
```

- Use the default Remote Debug Monitor if you are debugging a 32-bit process in a 32-bit virtual machine.

- (Optional) If you want to debug a 32-bit process in a 64-bit virtual machine, use the Remote Debug Monitor:

```
\Program Files (x86)\Microsoft Visual Studio 8\Common7\IDE\Remote
Debugger\x86\msvsmon.exe
```

- (Optional) If you want to debug a 64-bit process in a 64-bit virtual machine, use the 64-bit Remote Debug Monitor:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote
Debugger\x64\msvsmon.exe
```

- 4 Type a name for the Remote Debug Monitor on the guest.

The default name is VMDebug.

If a Remote Debug Monitor is already running on the guest, you can start another one with a different name or use one that is already running.

- 5 Choose the process you want to attach to from the list of available processes, and click **Attach**.
- 6 (Optional) If you want to refresh the list of running processes, click **Refresh**.

BETA

Glossary

- A** **administrative lockout**
A global setting providing password protection for Windows hosts. Administrative lockout restricts users from creating new virtual machines, editing virtual machine configurations, and changing network settings.
- B** **bridged networking**
A type of network connection between a virtual machine and the rest of the world. Under bridged networking, a virtual machine appears as an additional computer on the same physical Ethernet network as the host. *See also* [host-only networking](#).
- C** **clone**
A duplicate copy of a virtual machine. *See also* [full clone](#), [linked clone](#).
- configuration**
See [virtual machine configuration file](#).
- custom networking**
Any type of network connection between virtual machines and the host that does not use the default bridged, host-only, or network address translation (NAT) networking configurations. For instance, different virtual machines can be connected to the host by separate networks or connected to each other and not to the host. Any network topology is possible.
- D–E** **disk mode**
A property of a virtual disk that defines its external behavior (how the virtualization layer treats its data) but is completely invisible to the guest operating system. Available modes vary by product and include persistent mode (changes to

the disk are always preserved across sessions), nonpersistent mode (changes are never preserved), undoable mode (changes are preserved at the user's discretion), and append mode (similar to undoable, but the changes are preserved until a system administrator deletes the redo-log file).

drag-and-drop

With the drag and drop feature of Workstation, you can move files easily between a Windows or Linux host and a Windows, Linux, or Solaris virtual machine. You can drag and drop individual files or entire directories.

F Favorites list

A list in the left panel of the main Workstation screen that shows the names of virtual machines that a user has added to the list. The **Favorites** list makes it easy to launch a virtual machine or to connect to the virtual machine's configuration file in order to make changes in the virtual machine settings.

full clone

A complete copy of the original virtual machine plus all associated virtual disks. *See also* [linked clone](#).

full screen mode

A display mode in which the virtual machine's display fills the entire screen. *See also* [full screen switch mode](#).

full screen switch mode

A display mode in which the virtual machine's display fills the entire screen, and the user has no access to the VMware Workstation user interface. The user cannot create, reconfigure, or launch virtual machines. A system administrator performs these functions. *See also* [full screen mode](#).

G Go to Snapshot command

The **Go to Snapshot** command allows you to restore any snapshot of the active virtual machine. *See also* [revert to snapshot](#).

guest operating system

An operating system that runs inside a virtual machine. *See also* [“host operating system”](#) on page 495.

H–K headless

Describes a program that runs in the background without any interface connected to it. A running virtual machine that has no console connections is running headless.

host-only networking

A type of network connection between a virtual machine and the host. Under host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network. *See also* [bridged networking](#), [custom networking](#), [network address translation \(NAT\)](#).

host machine

The physical computer on which the VMware Workstation software is installed. It hosts the VMware Workstation virtual machines.

host operating system

An operating system that runs on the host machine. *See also* [guest operating system](#).

independent disk

A type of virtual disk that is not affected by snapshots. You can configure independent disks in persistent and nonpersistent modes. *See also* [nonpersistent mode](#), [persistent mode](#), [snapshot](#).

L–M**LAN segment**

A private virtual network that is available only to virtual machines within the same team. *See also* [virtual network](#), [team](#).

linked clone

A copy of the original virtual machine that shares the virtual disks with the original virtual machine in an ongoing manner. *See also* [full clone](#).

lockout

See [administrative lockout](#).

N–O**network address translation (NAT)**

A type of network connection that allows you to connect your virtual machines to an external network when you have only one IP network address, and that address is used by the host computer. If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

New Virtual Machine wizard

A point-and-click interface for convenient, easy creation of a virtual machine configuration. It creates files that define the virtual machine, including a virtual machine configuration file and (optionally) a virtual disk or physical disk file. *See also* [virtual machine settings editor](#).

NIC (network interface card)

An expansion board that provides a dedicated connection between a computer and a network. Also called a “network adapter.”

nonpersistent mode

A disk mode in which all disk writes issued by software running inside a virtual machine appear to be written to the independent disk but are in fact discarded after the virtual machine is powered off. As a result, a virtual disk or physical disk in independent-nonpersistent mode is not modified by activity in the virtual machine. *See also* [disk mode](#), [persistent mode](#).

P**parent**

The source or “original” virtual machine from which you take a snapshot or make a clone. A full clone has no continued link to its parent, but a linked clone and a snapshot each depend on the parent in an ongoing manner. If you delete the parent virtual machine, any linked clone or snapshot becomes permanently disabled. To prevent deletion, you can create a template virtual machine. *See also* [full clone](#), [linked clone](#), [snapshot](#), [template](#).

persistent mode

A disk mode in which all disk writes issued by software running inside a virtual machine are immediately and permanently written to a virtual disk that has been configured as an independent disk. As a result, a virtual disk or physical disk in independent-persistent mode behaves like a conventional disk drive on a physical computer. *See also* [disk mode](#), [nonpersistent mode](#).

physical disk

A hard disk in a virtual machine that is mapped to a physical disk drive or a partition of a drive on the host machine. A physical disk is also referred to as a raw disk. A virtual machine's disk can be stored as a file on the host file system or on a local hard disk. When a virtual machine is configured to use a physical disk, VMware Workstation directly accesses the local disk or partition as a physical device (not as a file on a file system). It is possible to boot a previously installed operating system on an existing partition within a virtual machine environment. The only limitation is that the existing partition must reside on a local IDE or SCSI drive. *See also* [virtual disk](#).

Q **quick switch mode**

A display mode in which the virtual machine's display fills most of the screen. In this mode, tabs at the top of the screen allow you to switch quickly from one running virtual machine to another. *See also* [full screen mode](#).

R **raw disk**

See [physical disk](#).

record/replay feature

This feature lets you record all of a Workstation 5 or 6 virtual machine's activity over a period of time. Unlike Workstation's movie-capture feature, the record/replay feature lets you exactly duplicate the operations and state of the virtual machine throughout the time of the recording.

redo log

The file that stores changes made to a disk in all modes except the persistent and independent-persistent modes. For a disk in nonpersistent mode, the redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk. You can permanently apply the changes saved in the redo log to a disk in undoable mode so that they become part of the main disk files. *See also* [disk mode](#).

resume

Return a virtual machine to operation from its suspended state. When you resume a suspended virtual machine, all applications are in the same state they were when the virtual machine was suspended. *See also* [suspend](#).

revert to snapshot

Reverting to a snapshot restores the status of the active virtual machine to its immediate parent snapshot. This parent is represented in the snapshot manager by the snapshot appearing to the immediate left of the **You Are Here** icon. *See also* [Go to Snapshot command](#), [snapshot manager](#), [You Are Here \(icon\)](#).

S **shared folder**

A shared folder is a folder on the host computer—or on a network drive accessible from the host computer—that can be used by both the host computer and one or more virtual machines. It provides a simple way of sharing files between host and guest or among virtual machines. In a Windows virtual machine, shared folders appear as folders on a designated drive letter. In a Linux or Solaris virtual machine, shared folders appear under a specified mount point.

snapshot

A snapshot preserves the virtual machine just as it was when you took that snapshot. This includes whether the virtual machine was powered on, powered off, or suspended. If the virtual hard disks are not set to independent mode, a snapshot also includes the state of the data on all the virtual machine's disks. Workstation lets you take snapshots of a virtual machine at any time and revert to that snapshot at any time. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. *See also* [independent disk](#).

snapshot manager

The snapshot manager is a window that allows you to take actions on any of the snapshots and recordings associated with the selected virtual machine. *See also* [record/replay feature](#), [snapshot](#).

suspend

Saves the current state of a running virtual machine. To return a suspended virtual machine to operation, you use the resume feature. *See also* [resume](#).

T–U**team**

A group of virtual machines that are configured to operate as one object. You can power on, power off, and suspend a team with one command. You can configure a team to communicate independently of any other virtual or real network by setting up a LAN segment. *See also* [LAN segment](#), [virtual network](#).

template

A virtual machine that cannot be deleted or added to a team. Setting a virtual machine as a template protects any linked clone or snapshots from being disabled inadvertently. *See also* [linked clone](#), [parent](#), [snapshot](#).

undoable mode

In VMware ESX Server 2.x, a disk mode in which all write operations issued by software running inside the virtual machines appear to be written to the disk but are in fact stored in a temporary file (.REDO) for the duration of the session. When the virtual machine is powered off, the user has three choices: permanently apply all changes to the disk; discard the changes, thus restoring the disk to its previous state; or keep the changes, so that further changes from future sessions can be added to the log. *See also* [disk mode](#).

unity mode

A display mode in which a virtual machine's applications are displayed in application windows directly on the host's desktop. The virtual machine console

view is hidden, and you can minimize the Workstation window. In this mode, a virtual machine's applications look just like other application windows on the host.

V–X **virtual disk**

A file or set of files appearing as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure a virtual machine with a virtual disk, you can install a new operating system into the disk file without the need to repartition a physical disk or reboot the host. *See also* [physical disk](#).

virtual hardware

The devices that make up a virtual machine. The virtual hardware includes the virtual disk, removable devices such as the DVD-ROM/CD-ROM and floppy drives, and the virtual Ethernet adapter. You configure these devices with the virtual machine settings editor. *See also* [virtual machine settings editor](#).

virtual machine

A virtualized x86-compatible PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host machine concurrently.

virtual machine configuration

The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine and how they are mapped to host files and devices.

virtual machine configuration file

A file containing a virtual machine configuration. It is created by the New Virtual Machine wizard. It is used by VMware Workstation to identify and run a specific virtual machine.

virtual machine settings editor

A point-and-click editor used to view and modify the settings of a virtual machine after its initial creation. *See also* [New Virtual Machine wizard](#).

virtual network

A network between virtual machines with no dependence on real-world hardware connections. For example, you can create a virtual network between a virtual machine and a host that has no external network connections. You can also create a LAN segment for communications between virtual machines on a team. *See also* [LAN segment](#), [team](#).

virtual network editor

A point-and-click editor used to view and modify the networking settings for the virtual networks created by VMware Workstation.

VMware Player

Free software that enables PC users to easily run any virtual machine on a Windows or Linux PC. VMware Player runs virtual machines created by VMware Workstation, VMware Server, or ESX Server and also supports Microsoft virtual machines and Symantec Backup Exec System Recovery disk formats.

VMware Tools

A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools control panel and support for such features as shared folders, drag-and-drop, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the virtual machine is running. *See also* [drag-and-drop](#), [shared folder](#).

Y–Z You Are Here (icon)

A special icon appearing in the snapshot manager that indicates the current status of the active virtual machine. This can be important when deciding whether to revert to, or go to a snapshot. *See also* [snapshot manager](#), [revert to snapshot](#), [Go to Snapshot command](#).

Index

Numerics

3D support **308**

A

About tab

 VMware Tools **126**

 VMware Workstation **43**

access control policies

 Active Directory password change
 proxying **381**

 setting **374**

ACE 2

 See VMware ACE 2

ACE instance

 defined **368**

 device connection policy **392**

 encryption **423**

 installing on a Linux host **446**

 installing on a Windows host **441**

 offline usage **400**

 removable device policy **392**

 running a Pocket ACE **439**

 setting policies for **374**

 uninstalling from a Linux host **447**

 uninstalling from a Windows
 host **444**

ACE Management Server

 and Active Directory password
 change proxying **381**

 defined **368**

ACE package

 See package

ACE Resources directory **423**

ACE tools, using **450**

ACE-enabled virtual machine

 configuring **424**

 creating multiple packages **426**

 defined **368**

 deployment **423**

ACPI **365**

ACPI S1 sleep feature **365**

activation policy **374**

Active Directory password change
 proxying **381**

adapter

 host virtual adapters **275**

 in promiscuous mode on a Linux
 host **292**

 virtual Ethernet **268**

adding notes to package history **431**

address

 assigning IP **279**

 assigning MAC manually **283**

 IP in virtual machine **89**

 IP on virtual network **277**

 MAC **282**

 network address translation **292**

 using DHCP to assign **278**

administrative lockout **351**

administrative tools policy **399**

AMD Athlon 64 processor **26, 38**

AMD Opteron processor **26, 38**

AMD Sempron processor **26, 38**

AMD Turion 64 processor **26, 38**

appliance view **395**

- appliance view for virtual machines **169**
- assign
 - IP address **277**
 - network port number in NAT **300**
- Athlon 64 processor **26, 38**
- attaching to a process
 - for debugging **473, 491**
- audio **35, 310, 311**
- AudioPCI **311**
- authentication policy **374**
- automatic bridging **270**

B

- background, running virtual machines
 - in **81, 238**
- bandwidth
 - controlling, in team networks **245**
 - LAN segment **255**
- battery information, reporting in
 - guest **158**
- BIOS
 - file in virtual machine **100**
 - provided in virtual machine **33**
- .bmp files for screen captures **171**
- bridged networking
 - configuring options **269**
 - defined **493**
- browser
 - and appliance views **169**
 - configuring on Linux host **45**
- BSD
 - supported 32-bit guest operating systems **37**
 - supported 64-bit guest operating systems **37**
- BT/KT-958 drivers **90**
- BusLogic **34, 343**

C

- capacity, disk **214, 226**

- .png files for screen captures **171**
- capture
 - snapshot of virtual machine **189**
 - virtual machine activity **233**
- CD
 - adding drive to virtual machine **227**
 - CD-ROM image file **33**
 - legacy emulation mode for **228**
- CD package delivery **430**
- .cfg file **100**
- change
 - team name **248**
 - virtual machine name **74**
- Change Version wizard **57**
- changing deployment platform for an
 - ACE-enabled virtual machine **423**
- changing the JVM path **469**
- clock
 - real-time on Linux host **45**
 - synchronize guest and host **122**
- clone
 - creating clone in New Team wizard **246, 251**
 - MAC address and UUID **201**
 - moving linked clones **209**
 - network identity **204**
 - overview **201**
 - virtual machine in a team **257**
- clone template **203**
- clones
 - creating in Clone Virtual Machine wizard **203**
 - enable template mode **203**
 - full **202**
 - IP address **204**
 - linked **202**
 - static IP address **204**
- cmd command for VMware Tools **135**

- color
 - display on VNC clients **167**
 - screen, in a virtual machine **307**
- comm port
 - See serial connection, serial port
- command-line interface
 - for VMware Tools **133**
 - for Workstation **455**
 - vmrun **457**
- commands
 - keyboard shortcuts **82**
 - startup, on the command line **455**
 - startup, on Windows hosts **456**
- configuration pages **485**
- configuration properties
 - setting post-debug event properties **488**
 - setting pre-debug event properties **488**
 - setting virtual machine properties **487**
- configurations
 - creating **485**
 - creating to attach to applications **471**
 - creating to start applications **469**
 - deleting **472**
 - duplicating to attach to applications **471**
 - duplicating to start applications **469**
 - editing to attach to applications **471**
 - editing to start applications **469**
 - managing **469, 485**
 - removing **489**
 - renaming **489**
- configuring
 - ACE-enabled virtual machine **424**
- connect
 - CD/DVDs and floppies to ISO images **230**
 - USB devices **337**
- Conversion wizard **137**
- Converter Import wizard **146, 147**
- converting virtual machines **137**
- copy protection policy **383**
- copy virtual machine **207**
- copyright information for Workstation **126**
- CPU
 - host requirement **26**
 - provided in virtual machine **32**
- creating
 - packages **426**
 - policies for an ACE instance **374**
- creating a virtual disk **219**
- Creative Labs **311**
- Creative Labs Sound Blaster **35**
- Ctrl+Alt **325**
- custom EULA package setting **422**
- D**
- DDNS **285**
- debugging
 - attaching to processes in a virtual machine **473, 491**
 - starting applications in virtual machine without **473**
 - starting in a virtual machine **472, 490**
 - using serial connection **322**
- default scripts for VMware Tools **127**
- defragmenting virtual disks **217**
- defragmenting virtual disks, before shrinking **218**
- deleting
 - configurations **472**
 - recordings **197**
 - recordings of virtual machine activity **241**
 - snapshots **193, 197**

- virtual machines **153**
- deploying packages **426**
- deployment
 - platform setting **423**
- deployment settings
 - instance customization, specifying **417**
- deployment tools
 - See Microsoft Sysprep deployment tools
- destinations for imported virtual machines **144**
- device connection policy **392**
- device connection, ACE instance **392**
- device drivers
 - for generic SCSI devices **344**
 - for USB support **339**
 - VMware Tools **104**
- device, removable, policy **392**
- device, USB **393**
- devices
 - adding a generic SCSI device **345, 346**
 - connecting and disconnecting **124, 166**
 - disconnecting from USB controller **341**
 - processor **32**
 - USB **335**
- Devices tab
 - in Preferences dialog box **78**
 - VMware Tools **124**
- DHCP
 - assigning IP addresses on a virtual network **278**
 - changing settings **272, 275**
 - configuring on a Linux host **279**
 - configuring on a Windows host **279**
 - DHCPD **285**
 - lease **274**
 - on a virtual network with NAT **293**
 - server **260, 274**
 - server on virtual network **263, 264**
 - stopping **290**
- dial-up connection **280**
- directories
 - mounting shared, on Linux **182**
 - viewing shared, on Solaris guests **182**
 - viewing shared, on Windows guests **181**
- disable
 - acceleration **166**
 - copying and pasting text and files **177**
 - drag-and-drop of files and folders **176**
 - folder sharing **178**
 - interface features **351**
- disc labels for packages **430**
- disk
 - See *also* virtual disk
 - IDE drive supported in host **27**
 - IDE drives in virtual machine **33**
 - IDE optical drive supported in host **27**
 - independent **192**
 - SCSI drive supported in host **27**
 - SCSI optical drive supported in host **27**
 - size **214, 226**
 - space required on host computer **27**
 - .vmdk virtual disk file **100**
- disk space required for packaging **428**
- display
 - color depth **307**
 - fitting window to virtual machine **163**
 - full screen **156**

- multiple monitor **160, 162**
- switching virtual machines **158**
- Display tab in preferences editor **163**
- distributing packages **426, 430**
- DMZ **245**
- DNS **293**
- DNS setup issues, troubleshooting **453**
- domain join
 - remote, setting up **420**
- domain setting, in instance customization
 - package settings **417**
- domain, problem with domain validation or name resolution **453**
- domain, problem with logging in after revert to installed **453**
- downgrading virtual machines **57**
- downloading Microsoft Sysprep deployment tools **417**
- drag and drop **175, 494**
- dragging and dropping files between host and guest **175**
- drive supported in host **27**
- driver
 - SCSI **343**
 - sound **311**
- drivers
 - video, in older versions of Windows **107**
- drives
 - See also* disk
 - tape **343**
- dual-boot computers and virtual machines **231**
- dual-monitor display **160, 162**
- DVD
 - adding drive to virtual machine **227**
 - legacy emulation mode for **228**
 - optical, supported **27**
- DVD package delivery **430**
- dynamic domain name service **285**

E

- Eclipse
 - installing the Workstation plug-in for **42**
- education services **23**
- EHCI controller **34**
- EM64T processor **27, 38**
- encryption
 - ACE instance protection **414**
 - package protection **414**
 - package setting **414**
- enhanced keyboard filter **396**
- enhanced virtual keyboard **324**
- Ethernet adapter
 - adding to virtual machine **268**
 - for teams **256**
 - promiscuous mode on a Linux host **292**
 - virtual network adapters **260**
- Ethernet switches **35**
- expiration policy **382**

F

- Favorites list
 - creating folders in **73**
 - defined **494**
 - overview **72**
 - pictured **72**
 - removing virtual machines from **74**
- files
 - BIOS in virtual machine **100**
 - redo log **100**
 - Samba and file sharing on a Linux host **305**
 - sharing among virtual machines and host **175**
 - snapshot **100**
 - suspended state **100**
 - used by a virtual machine **100**

- used by snapshot **100**
 - virtual machine **151**
- files, distribution formats for
 - package **430**
- firewall **301**
- fit
 - guest **163**
 - window **163**
 - window to virtual machine **163**
- floppy
 - drives in virtual machine **34**
 - image file **34, 230**
- floppy drive
 - adding to virtual machine **229**
- folders
 - in the Favorites list **73**
 - shared, *See* shared folder
- for displaying Workstation help **29, 32**
- FreeBSD
 - supported 32-bit guest operating systems **37**
 - supported 64-bit guest operating systems **37**
 - VMware Tools for **114**
- FTP **294**
- full screen mode
 - defined **494**
 - using **156**
- full screen switch mode **355**
 - log file **364**
- full screen toolbar **395**
- G**
 - gated host network **284**
 - global configuration file **356**
 - graphics
 - See also* display
 - support in virtual machine **33, 307**
 - guest

- autofit **163**
 - defined **26**
 - fit **163**
- Guest network access policies
 - interactions with tunneling protocols **392**
- guest network access policies **384**
- guest operating system
 - defined **494**
 - for instance customization **416**
 - installing **96**
 - support for 64-bit **38**
 - supported **35**
 - supported FreeBSD 32-bit **37**
 - supported FreeBSD 64-bit **37**
 - supported Linux 32-bit **37**
 - supported Linux 64-bit **37**
 - supported MS-DOS **36**
 - supported Solaris 32-bit **37**
 - supported Solaris 64-bit **37**
 - upgrades **99**
 - Windows 32-bit **36**
 - Windows 64-bit **36**
- GUID Partition Table (GPT) disks **143**

H

- Hardware tab in virtual machine settings editor **79**
- headless virtual machines (run in the background) **81, 238**
- help
 - configuring Web browser for **45**
- host
 - defined **26**
 - hard disk space required **27**
 - operating system, defined **495**
 - optical drives supported **27**
 - system requirements **26**
- host computer **495**

- Host network access policies
 - interactions with tunneling protocols **392**
- host policies **384, 441**
- host virtual adapters **275**
- host virtual network mapping **271, 272**
- host-guest data script policies **382**
- host-only networking
 - basic configuration **263**
 - defined **495**
 - selecting IP addresses **277**
- hot fix
 - policies **400**
 - responding **452**
- hot keys
 - for full screen switch mode **358, 359**
 - in Workstation preferences **325**
- Hot Keys tab **78**
- I**
- ICMP **294**
- IDE
 - drive supported in host **27**
 - drives in virtual machine **33**
 - optical drive supported in host **27**
- IDESCSI, setting up virtual disk as **215**
- image file
 - floppy **34, 230**
 - ISO **33, 227, 230**
- importing virtual machines **137, 139**
- independent disk **192**
- initialization scripts for instance
 - customization package settings **417**
- install
 - guest operating system **96**
 - on Linux host **45**
 - on Windows host **41**
 - silent **43, 108**
 - software in a virtual machine **165**
- installing
 - ACE instance on a Linux host **446**
 - ACE instance on a Windows host **441**
 - Pocket ACE on portable device **437**
 - VMware Player on a Linux host **445**
- instance customization
 - enabled, packaging overview **430**
 - guest operating systems for **416**
 - initialization scripts **417**
 - Microsoft Sysprep deployment tools **416**
 - package settings, overview **415**
 - placeholder values **419**
 - specifying deployment settings **417**
 - specifying license information for Windows server products **420**
 - workgroup or domain setting **417**
- Intel EM64T processor **27, 38**
- lomega
 - parallel port zip drives **314**
- IP address
 - assigning **279**
 - clone **204**
 - in virtual machine **89**
 - static **278**
- IP forwarding **280**
- IP packet forwarding
 - disabling **281**
- ISO image file **33, 227, 230**
- J**
- JVM
 - automatically selected **469**
 - changing the path **469**

K

- kpbs, for LAN segment **255**
- kernel
 - paravirtual, support for **98**
 - upgrades, and Workstation **47**
- key code mapping **329**
- keyboard
 - enhanced virtual, on Windows **324**
 - language keymaps for VNC clients **325**
 - mapping on a Linux host **327**
 - shortcuts **82**
 - USB **335**
- keyboard, enhanced filter **396**
- keyloggers **396**
- keysym
 - defined **329**
 - mapping **329**
- knowledge base, VMware **20**

L

- LAN segment
 - and teams **254**
 - deleting **256**
- LAN segments
 - changing name **255**
 - configuring connections to **256**
 - setting bandwidth **255**
 - setting Kbps **255**
 - setting packet loss **255**
- launch configurations **469**
 - creating to attach to applications **471**
 - creating to start applications **469**
 - duplicating to attach to applications **471**
 - duplicating to start applications **469**
 - editing to attach to applications **471**
 - editing to start applications **469**

leak

- IP packets in a virtual machine **280**
- IP packets in host-only network **280**

legacy emulation for DVD/CD-ROM drives **228**

legacy virtual machine

creating **87**

licensing, serial number and **42**

linked clone

moving **209**

Linux

- installing on Linux host **45**
- supported 32-bit guest operating systems **37**
- supported 64-bit guest operating systems **37**
- supported host operating systems **29**
- uninstalling Workstation on Linux host **48**
- upgrading on Linux host **55**
- VMware Tools for **110**

Linux 64-bit host **30**

LiveState system image, importing **139**

location of virtual machine files **88, 151**

lock files **214**

lockout

for some interface features **351**

Workstation preference **78**

.log file **100**

log files **364**

LSI Logic **33**

ISI Logic **90, 343**

M**MAC address**

and clones **201**

assigning manually **283**

of virtual Ethernet adapter **282**

map

- key code **329**
 - keyboard **327**
 - keysym **329**
 - mapped drives, for virtual disks **184**
 - master boot record (MBR) disks **143**
 - memory
 - amount required on host **27**
 - available in virtual machine **33**
 - memory settings **395**
 - Microsoft Sysprep deployment tools
 - downloading **417**
 - MIDI **310**
 - migrate
 - virtual machine **209**
 - mode
 - full screen **156, 494**
 - quick switch **158, 497**
 - modifier keys **358**
 - monitors
 - specifying the number of **160, 162**
 - using multiple **160, 162**
 - mouse
 - driver, installed by VMware Tools **104**
 - USB **335**
 - movie capture **171**
 - moving a virtual machine **205**
 - MP3 **310**
 - MS-DOS **36**
 - multiple monitors, using **160, 162**
 - Mylex **34, 90, 343**
- N**
- name
 - changing team name **248**
 - changing virtual machine name **74**
 - named pipe **319**
 - NAT
 - advanced configuration **295**
 - and DHCP **293**
 - and DNS **293**
 - and the host computer **293**
 - defined **495**
 - external access from a NAT network **294**
 - on virtual network **262, 292**
 - port forwarding **300, 304, 305**
 - sample configuration file for Linux host **303**
 - selecting IP addresses **277**
 - specifying connection from port below 1024 **297**
 - when creating a virtual machine
 - NAT.conf **297, 303**
 - NetLogon **301**
 - NetWare, Novell **37, 116, 126**
 - network
 - adding and modifying virtual Ethernet adapters **268**
 - automatic bridging **270**
 - bridged networking **493**
 - changing DHCP settings **272, 275**
 - changing subnet settings **272, 275**
 - changing the configuration **267**
 - components **259**
 - configuring bridged networking options **269**
 - custom networking **493**
 - DHCP **278**
 - DHCP server **260**
 - dial-up connection **280**
 - dynamic domain name service **285**
 - hardware address **282**
 - host virtual network mapping **271, 272**
 - host-only **263, 495**
 - host-only subnet **278**
 - identity, clone **204**
 - IP forwarding **280**

- IP packet leaks **280**
- locking out access to settings **351**
- MAC address **282**
- NAT **262, 292, 495**
- NAT as firewall **301**
- NAT subnet **278**
- packet filtering **281**
- promiscuous mode on a Linux host **292**
- routing between two host-only networks **290**
- Samba **305**
- second bridged network on a Linux host **286**
- switch **259**
- token ring **263**
- two host-only networks **286**
- virtual DHCP server **263, 264**
- virtual Ethernet adapter **260**
- virtual network editor **270, 276, 279, 500**
- virtual switch **259**
- virtualizing in a team **245**
- network access policies **384**
- network adapters
 - creating, for team networks **256**
- network address translation
 - See NAT
- network image package delivery **430**
- New Package wizard **426**
- New Virtual Machine wizard **75, 92, 94, 213, 496**
- NFS ports **297**
- Novell NetWare
 - supported guest operating systems **37**
 - VMware Tools for **116**
- Novell Open Enterprise Server
 - supported guest operating systems **37**
- NVRAM **100**

O

- offline usage of ACE instances, policy **400**
- Open Enterprise Server **37**
- open virtual machine format (.ovf and .ova files) **142**
- operating system
 - 32-bit Windows host **28**
 - 64-bit Windows host **29**
 - FreeBSD 32-bit guest **37**
 - FreeBSD 64-bit guest **37**
 - guest **494**
 - host, defined **495**
 - installing guest **96**
 - Linux 32-bit guest **37**
 - Linux 32-bit host **30**
 - Linux 64-bit guest **37**
 - Linux 64-bit host **31**
 - MS-DOS guest **36**
 - Solaris 32-bit guest **37**
 - Solaris 64-bit guest **37**
 - support for 64-bit guest **38**
 - Windows 32-bit guest **36**
 - Windows 64-bit **36**
- Opteron processor **26, 38**
- optical drive supported in host **27**
- Options tab
 - virtual machine settings editor **80**
 - VMware Tools **122**
- .ovf and .ova files **142**

P

- P2V (physical-to-virtual) conversion **137**
- package
 - burning files onto discs **430**
 - changing lifetime setting **414**
 - creating **426**
 - creating multiple **426**
 - creation progress **430**
 - deployment for Pocket ACE **437**

- deployment platform for **423**
 - disc labels **430**
 - disk space required **428**
 - distribution format, selecting **430**
 - encryption **423**
 - format of files **430**
 - history **431**
 - Pocket ACE installation **437**
 - pre-deployment test **431**
 - previewing before deployment **431**
 - registration **430**
 - testing before deployment **431**
- package lifetime package setting **414**
- package properties dialog box **431**
- package settings
 - custom EULA **422**
 - deployment platform **423**
 - encryption **414**
 - instance customization,
 - overview **415**
 - package lifetime **414**
 - placeholder values in instance
 - customization **419**
 - remote domain join **420**
 - workgroup or domain in instance
 - customization **417**
- packaging
 - burning files onto discs **430**
 - creation progress **430**
 - disk space required **428**
 - select distribution format **430**
 - with instance customization
 - enabled **430**
- packet
 - filtering **281**
 - leaks **280**
- packet loss, configuring, for LAN
 - segments **255**
- parallel ports
 - and lomega zip drives **314**
 - and the Linux kernel **315**
 - configuring on a Linux host **314**
 - in a virtual machine **313**
 - installing in virtual machines **313**
- paravirtualized kernels in Linux
 - guests **98**
- parent
 - snapshot **190**
- passwords
 - and administrative lockout **351**
 - removing forgotten password **352**
- performance
 - debugging mode **242**
- physical disk
 - adding physical disks **221**
 - capacity **216**
 - defined **496**
 - storing virtual disks on **215**
 - using in a virtual machine
- ping **294**
- pipe, named **319**
- placeholder values in instance
 - customization package
 - settings **419**
- platform deployment setting **423**
- Player policy **395**
- plug-ins, writing **402**
- .png files for screen captures **171**
- Pocket ACE
 - correct time necessary on host
 - computers **439**
 - description **91, 435**
 - Disk Size Calculator **91**
 - installing on portable device **437**
 - portable device requirements **435**
 - running **439**
- policies
 - access control **374**

- activation **374**
 - administrative tools **399**
 - authentication **374**
 - copy protection **383**
 - device connection **392**
 - expiration **382**
 - host **384, 441**
 - host-guest data script **382**
 - hot fix **400**
 - network access **384**
 - Player runtime **395**
 - removable device **392**
 - resource signing **383**
 - runtime preferences **395**
 - setting for an ACE instance **374**
 - snapshot **398**
 - update frequency **400**
 - USB device **393**
 - using scripts **402**
 - policy editor, using **374**
 - policy update frequency **400**
 - port
 - TCP and UDP below 1024 **297**
 - VNC **167**
 - port forwarding **300, 304, 305**
 - Power menu
 - disable functions **352**
 - using, for teams **254**
 - power off
 - snapshot options **197**
 - team **253**
 - Power Off button **152**
 - power on
 - a virtual machine **150**
 - team **253**
 - Powered On list **74**
 - power-on script **378**
 - preferences
 - display **163**
 - hot keys **325**
 - setting, for Workstation **76**
 - workspace **77**
 - Preview in Player icon **425**
 - preview mode
 - test **425**
 - viewing ACE instances before deployment **431**
 - previewing packages **431**
 - processor
 - host requirement **26**
 - provided in virtual machine **32**
 - supported for 64-bit guest **26, 38**
 - promiscuous mode **292**
 - properties
 - setting post-debug event **488**
 - setting pre-debug event **488**
 - setting virtual machine **487**
 - publishing policy changes **431**
- ## Q
- quick switch mode **158, 497**
 - quiet mode, install VMware Tools **108**
 - quit, VMware Player **449**
- ## R
- RAM
 - amount required on host **27**
 - available in virtual machine **33**
 - raw disk
 - See physical disk
 - Real Media **310**
 - real-time clock requirement on Linux
 - host **45**
 - record/replay feature **233, 235**
 - recording
 - renaming **196**
 - recordings
 - deleting **197**

- .REDO file 100**
- registration **21**
- registration of packages **430**
- reimage snapshots **398**
- remote connections to a virtual machine **167**
- remote domain join
 - setting up **420**
- RemoteDisplay.vnc.keyMap
 - property **325**
- removable device **392**
- removable drive for Pocket ACE **437**
- removing
 - a virtual disk **221**
 - devices from a virtual machine **166**
 - Workstation 2 or 3 **52**
- Repair option
 - for VMware Tools installations **107**
- repairing VMware Tools
 - installations **117, 120**
- Replay Last Recording button **235**
- Replay toolbar **236, 237**
- reporting problems to VMware **21**
- Reset button **153**
- resizing
 - Linux guests **164**
 - Solaris guests **164**
- resource signing policy **383**
- restricted user interface **352**
- resume
 - defined **497**
 - team **253**
 - virtual machine **187**
- reverting to snapshot **196**
- routing
 - between host-only networks **290**
 - host only **284**
- RPM installer for VMware
 - Workstation **46**
- runtime preferences policy **395**

S

- Samba
 - and file sharing on a Linux host **305**
 - modifying configuration for Workstation **305**
 - on both bridged and host-only networks **306**
- scan code **329**
- scanner **343**
- screen captures **171**
- screen colors
 - for VNC clients **167**
 - setting, for virtual machines **307**
- screen modes
 - full screen **156**
 - quick switch **158**
- screen resolution **165**
- .png files for screen captures **171**
- screenshots **171**
- script, power on **378**
- scripts
 - creating custom VMware Tools **128**
 - enabling, disabling, and running **124**
 - for instance customization **417**
 - running and disabling **130**
 - running during power state changes **127**
 - writing **402**
- Scripts tab
 - VMware Tools **124**
- SCSI **27**
 - adding a generic SCSI device **345, 346**
 - avoiding concurrent access on a Linux host **344**
 - connecting to generic **343**
 - devices in virtual machine **33**
 - driver for Windows NT guest **344**
 - driver for Windows Server 2003

- guest **343**
 - driver for Windows XP guest **343**
 - drivers **90, 343**
 - generic SCSI on a Linux host **344**
 - generic SCSI on a Windows host **343**
 - permissions for a generic SCSI device on a Linux host **343**
 - setting up virtual disk as **215**
- Sempron processor **26, 38**
- serial connection
 - between host application and virtual machine **319**
 - between two virtual machines **320**
 - for debugging **322**
 - to a serial port on the host **318**
- serial number
 - for Workstation **42**
- serial port, installing and using **318**
- server
 - DHCP **260, 279, 293, 301**
 - DNS **285, 293, 294, 296**
 - WINS **295**
- setting
 - correct time on Pocket ACE host computers **439**
 - policies for an ACE instance **374**
- setting up
 - ACE-enabled virtual machine configuration **424**
 - packages **426**
- settings editor, virtual machine **499**
- share
 - drag and drop **494**
 - files on a Linux host with Samba **305**
- shared folder
 - defined **497**
 - enable and disable **178**
 - mounting, on Linux **182**
 - on Linux and Solaris guests **182**
 - permissions on Linux **182**
 - using **177**
 - viewing **181**
- Shared Folders tab
 - VMware Tools **125**
- sharing virtual machines **209**
- shortcut, desktop, for Workstation **42**
- shortcuts, keyboard **82**
- shrink
 - virtual disks **125, 218**
 - virtual disks in Netware **126**
- Shrink tab, VMware Tools **125**
- Sidebar panel **72**
- silent install **108**
- size
 - disk **214, 226**
 - virtual disk **33**
- sleep, ACPI **365**
- smart cards in virtual machines **342**
- SMP
 - See virtual SMP
- snapshot
 - and Workstation 4 virtual machines **198**
 - as background activity **192**
 - defined **498**
 - deleting **193, 197**
 - disabling menu functions **352**
 - excluding virtual disks from **192**
 - files **100**
 - linear process **189**
 - parent **190**
 - policies **398**
 - power-off options **197**
 - process tree **190**
 - renaming **193, 196**
 - restoring **196**
 - reverting to **196**

- reverting to at power off **196**
 - taking **195**
 - team **257**
 - using **189**
 - snapshot manager **193**
 - Solaris
 - resizing guests **164**
 - supported 32-bit guest operating systems **37**
 - supported 64-bit guest operating systems **37**
 - VMware Tools for **113**
 - sound
 - configuring **310**
 - drivers for Windows 9x and NT guests **311**
 - Sound Blaster **311**
 - support in guest **35**
 - .spf file, importing **139**
 - starting
 - applications in a virtual machine without debugging **473**
 - debugging session in a virtual machine **472, 490**
 - session in a virtual machine without debugging **490**
 - starting VMware Player **447**
 - starting Workstation **61**
 - startup commands
 - used by VMware Tools when starting virtual machines **132**
 - startup scripts
 - using VMware Tools **131**
 - static IP addresses
 - clone **204**
 - range of **293**
 - .std file **100**
 - stopping VMware Player **449**
 - StorageCraft images, importing **139**
 - subnet
 - changing settings **272, 275**
 - in NAT configuration **278**
 - on host-only network **278**
 - Sun Solaris
 - supported 32-bit guest operating systems **37**
 - supported 64-bit guest operating systems **37**
 - support scripts, running **21**
 - suspend
 - defined **498**
 - files **100**
 - team **253**
 - virtual machine **187**
 - .sv2i file, importing **139**
 - SVGA drivers
 - installing, in older Windows guests **107**
 - switch
 - virtual network **259**
 - workspaces in Linux guest **325**
 - symmetric multiprocessing
 - See virtual SMP
 - Sysprep deployment tools
 - See Microsoft Sysprep deployment tools
 - System requirements
 - local area networking **28**
 - system requirements **26**
 - display **27**
 - memory **27**
 - PC hardware **26**
- ## T
- tabs
 - in Preferences dialog box **77**
 - virtual machine **63**
 - tape drive **343**
 - .tar file for installing VMware Tools **111**

tar installer for VMware Workstation **46**

team

adding virtual machine to **251**

and LAN segments **254**

cloning virtual machine from **257**

closing **248**

creating clone in New Team
wizard **246, 251**

deleting **249**

Ethernet adapters for **256**

name change **248**

network **245**

new **246**

no clone template **203**

opening **247**

overview **245**

power off **253**

powering on **253**

removing virtual machine from **251**

resume **253**

snapshot **257**

suspend **253**

technical support resources **20**

Telnet **294**

template mode for clones **203**

testing a package **431**

testing package

pre-deployment **431**

3D support **308**

time synchronization **122**

time, synchronizing, between guest and
host **122**

time.synchronize options for VMware
Tools **123, 135**

token ring **263**

toolbar

customizing **70, 71**

hide **352**

training courses **23**

troubleshooting

responding to hot fix requests **452**

users' problems **372**

with vmware-acetool **450**

Turion 64 processor **26, 38**

U

UHCI controller **34**

uninstalling

an ACE instance from a Linux
host **447**

an ACE instance from a Windows
host **444**

host virtual adapters **275**

VMware Tools **120**

Workstation on Linux host **48**

Workstation on Windows host **44**

Unity mode **154**

update frequency **400**

updates, checking for Workstation **74**

upgrade

guest operating systems **99**

Linux kernel, reconfiguring Worksta-
tion after upgrade **47**

on Linux host **55**

on Windows host **53**

on Windows Vista host **54**

removing snapshots before virtual
machine upgrades **51**

virtual machines **57, 58**

VMware Tools **117**

VMware Workstation **51**

USB

connecting devices **337**

control of devices by host and
guest **340**

controller, enabling and
disabling **336**

devices in a virtual machine **335**

disconnecting devices **341**

- keyboard and mouse **335**
 - on a Linux host **339**
 - on a Windows host **338**
 - port specifications **34**
 - supported device types **335**
 - USB device connection **392**
 - USB device policy **393**
 - user groups, accessing **20**
 - user interface
 - overview **62**
 - restricted **352**
 - UUID (universal unique identifier)
 - and clones **201**
 - location **199**
 - options for when you move a virtual machine **200**
 - specifying **201**
- ## V
- VAssert API **173**
 - version information for Workstation **126**
 - version, changing virtual machine **57**
 - VGA **165**
 - viewing package history **431**
 - virtual adapter
 - host virtual adapters **275**
 - virtual appliances
 - open virtual machine format (OVF) **142**
 - virtual disk
 - See also* disk
 - adding to virtual machine **219, 220**
 - allocating disk space **91**
 - defined **214, 499**
 - defragmenting **217**
 - defragmenting before shrinking **218**
 - IDE, size **33**
 - legacy **231**
 - mapping drives to **184**
 - setting up as IDE or SCSI **215**
 - shrinking **125, 218**
 - shrinking in Netware **126**
 - size **33**
 - storing on physical disks **215**
 - using in a new virtual machine **87**
 - Virtual Disk Manager **231**
 - .vmdk file **100**
 - Virtual Disk Manager **231**
 - virtual hardware
 - CPU issues **147**
 - disk device issues **147**
 - Ethernet adapter issues **147**
 - graphics card issues **147**
 - virtual keyboard **324**
 - virtual machine **79**
 - adding a virtual disk **219, 220**
 - adding floppy drive **229**
 - adding or modifying an Ethernet adapter **268**
 - adding physical disk **221**
 - adding to team **251**
 - and SMP **348**
 - cloning from team **257**
 - constituent files **100**
 - creating **85, 103, 137**
 - creating a clone **203**
 - default location of **88**
 - defined **499**
 - delete **153**
 - files **151**
 - IDE drives in
 - installing software in **165**
 - migrating **209**
 - moving **199, 205**
 - moving SMP virtual machines **348**
 - name change **74**
 - platform specifications **32**
 - portability **214**

- power off vs. shut down **152**
- recording activity of **235**
- removing from Favorites list **74**
- removing from team **251**
- reset vs. restart **153**
- resuming **187**
- running in the background **81, 238**
- settings **79**
- shutting down **152**
- starting **149**
- starting in full screen mode **361**
- suspending **187**
- upgrade or downgrade **57**
- upgrading procedure **58**
- using snapshots **189**
- Virtual Machine Communication Interface (VMCI) **104**
- virtual machine settings editor
 - defined **499**
 - restricting access **351, 352**
- virtual machines
 - converting **137**
- virtual network editor **500**
- Virtual PC, importing **139**
- virtual SMP
 - moving SMP virtual machines **348**
 - using **348**
- virtual switch **259**
- virtual Symmetric Multiprocessing
 - See virtual SMP
- Visual Studio
 - installing the Workstation plug-in for **42**
- VIX API **173**
- .vmc file, importing **139**
- VMCI Sockets interface **173**
- .vmdk file **100**
- .vmem file **100**
- VMI (Virtual Machine Interface) enabled
 - kernels **98**
- VMnet1 **286**
- VMnet8 **293**
- vmrun **457**
- .vmsd file **100**
- .vmsn file **100**
- .vmss file **100**
- .vmtm file **100**
- VMware ACE 2
 - components **368**
 - described **367**
 - key features **368**
- VMware community forums **20**
- vmware-config.pl **47**
- VMware Converter **137, 139**
- VMware Player
 - installing on a Linux host **445**
 - quitting **449**
 - running **210**
 - sharing virtual machines with **210**
 - starting **447**
 - stopping **449**
- VMware Tools
 - About tab **126**
 - automated install **108**
 - command-line interface **133**
 - configuring **121**
 - configuring in a Netware virtual machine **126**
 - control panel **121**
 - defined **500**
 - device drivers **104**
 - Devices tab **124**
 - for FreeBSD guests **114**
 - for Linux guests **110**
 - for NetWare guests **116**
 - for Solaris guests **113**
 - installing from the command line with the RPM installer **111**

- installing from the command line
 - with the tar installer **111**
 - installing on Windows guests **106**
 - modifying installation **120**
 - Options tab **122**
 - running scripts during power state changes **127**
 - Scripts tab **124**
 - Shared Folders tab **125**
 - Shrink tab **125**
 - silent install **108**
 - taskbar icon, displaying **122**
 - uninstalling **120**
 - updating **117**
 - using from command line **126**
 - VMware user process **105**
 - vmwtool commands **126**
 - VMware Tools service
 - executing commands on halt or reboot **130**
 - overview of **104**
 - passing strings from the host **131**
 - VMware Tools update option **117**
 - VMware user process, in VMware Tools **105**
 - vmware-user, starting manually **117**
 - vmware-acetool, using **450**
 - VMware-config.pl file **46**
 - vmware-fullscreen log file **364**
 - vmwtool **126**
 - .vmx file **100**
 - .vmxf file **100**
 - VNC
 - setting a keyboard map for **325**
 - setting a virtual machine to act as a VNC server **167**
 - VProbes **173**
 - v-scan code
 - defined **329**
 - table of codes **331**
- ## W
- .wav file **310**
 - window
 - autofit **163**
 - fit **163**
 - window size **165**
 - Windows
 - 32-bit guest operating systems **36**
 - 64-bit guest operating systems **36**
 - uninstalling on Windows host **44**
 - upgrading on Windows host **53**
 - upgrading to Windows Vista **54**
 - VMware Tools for **106**
 - Windows 95 sound driver **311**
 - Windows 98 sound driver **311**
 - Windows NT
 - SCSI driver for guest **344**
 - sound driver **311**
 - Windows Server 2003
 - SCSI driver for guest **343**
 - Windows XP
 - SCSI driver for guest **343**
 - wizard
 - New Package **426**
 - New Team **246**
 - New Virtual Machine **75, 92, 94, 496**
 - Workspace tab in preferences editor **77**
 - workspaces
 - location of **77**
 - switching in Linux guest **325**
 - Workstation
 - checking for updates for **74**
 - serial number for **42**
 - starting **61**

X

X server and keyboard mapping **327**

X toolkit options **456**

xFree86 and keyboard mapping **327**

Z

zip drives

 disconnecting **341**

 on a parallel port **314**

BETA